

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

10542 U.S. PTO
09/628108
09/27/86

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application:

1999年 9月29日

出 願 番 号
Application Number:

平成11年特許願第277265号

出 願 人
Applicant(s):

株式会社日立製作所

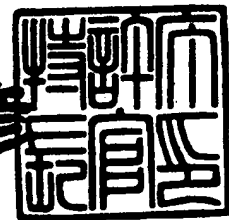
T. Fujiyama et al
filed 7-27-00
703-684-1120
Tsm-13

CERTIFIED COPY OF
PRIORITY DOCUMENT

2000年 5月12日

特許庁長官
Commissioner,
Patent Office

近 藤 隆 彦



出証番号 出証特2000-3033830

HT 150901

【書類名】 特許願

【整理番号】 HL12573000

【提出日】 平成11年 9月29日

【あて先】 特許庁長官 殿

【国際特許分類】 G06F 9/06

【発明者】

【住所又は居所】 神奈川県川崎市麻生区王禅寺 1 0 9 9 番地 株式会社日立製作所 システム開発研究所内

【氏名】 藤山 達也

【発明者】

【住所又は居所】 神奈川県川崎市麻生区王禅寺 1 0 9 9 番地 株式会社日立製作所 システム開発研究所内

【氏名】 萱島 信

【発明者】

【住所又は居所】 神奈川県川崎市麻生区王禅寺 1 0 9 9 番地 株式会社日立製作所 システム開発研究所内

【氏名】 永井 康彦

【発明者】

【住所又は居所】 神奈川県川崎市幸区鹿島田 8 9 0 番地 株式会社日立製作所 情報システム事業部内

【氏名】 角田 光弘

【発明者】

【住所又は居所】 神奈川県川崎市幸区鹿島田 8 9 0 番地 株式会社日立製作所 情報システム事業部内

【氏名】 山田 知明

【特許出願人】

【識別番号】 000005108

【氏名又は名称】 株式会社 日立製作所

【代理人】

【識別番号】 100087170

【弁理士】

【氏名又は名称】 富田 和子

【手数料の表示】

【予納台帳番号】 012014

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】明細書

【発明の名称】セキュリティ評価方法および装置、セキュリティ施策の作成支援方法および装置

【特許請求の範囲】

【請求項 1】

電子計算機を用いて、1以上の機器で構成されるシステムに施されたセキュリティを評価するセキュリティ評価方法であって、

前記電子計算機に接続された入力装置を介して、操作者より、評価対象システムと当該システムを構成する各機器の指定を受け付ける第1のステップと、

システムタイプ毎に、構成機器と当該構成機器に施すべきセキュリティ施策とが記述されたデータベースを検索し、前記第1のステップで指定された評価対象システムに対応するシステムタイプの構成機器のうち、前記第1のステップで指定された評価対象システムを構成する各機器に施すべきセキュリティ施策を読み出す第2のステップと、

前記第1のステップで指定された評価対象システムを構成する機器毎に、前記第2のステップで読み出したセキュリティ施策を対応付けて、前記電子計算機に接続された表示装置に表示し、前記入力装置を介して、操作者より、当該機器毎に対応付けて表示されたセキュリティ施策の実施の有無を受け付ける第3のステップと、

前記第3のステップで受け付けた評価対象システムを構成する各機器のセキュリティ施策の実施の有無に基づいて、当該評価対象システムに施されたセキュリティ状態の評価を行ない、その結果を前記表示装置に表示する第4のステップと、を有すること

を特徴とするセキュリティ評価方法。

【請求項 2】

請求項 1 記載のセキュリティ評価方法であって、

前記データベースは、記述されているセキュリティ施策各々に、そのセキュリティ施策を施すことによって確保されるセキュリティの種類が対応付けられて記述されており、

前記第 4 のステップは、前記第 2 のステップで読み出した評価対象システムを構成する各機器のセキュリティ施策を、当該セキュリティ施策に対応付けられたセキュリティの種類毎に分類し、セキュリティの種類毎に、当該種類に分類されたセキュリティ施策の数に対する前記第 3 のステップで実施有りとされたセキュリティ施策の数の割合を求め、これを当該種類に対するセキュリティ施策の達成度として、セキュリティの種類各々の達成度を前記表示装置に表示すること

を特徴とするセキュリティ評価方法。

【請求項 3】

請求項 1 記載のセキュリティ評価方法であって、

前記データベースは、記述されているセキュリティ施策各々に、そのセキュリティ施策を施すことによって確保されるセキュリティの種類とそのセキュリティ施策を施すことによって回避される危険度とが併せて記述されており、

前記第 4 のステップは、前記第 2 のステップで読み出した評価対象システムを構成する各機器のセキュリティ施策を、当該セキュリティ施策に対応付けられたセキュリティの種類毎に分類し、セキュリティの種類毎に、当該種類に分類されるセキュリティ施策のうち、前記第 3 のステップで実施無しとされたセキュリティ施策に対応付けられた危険度の総和を求め、これを当該種類に対するセキュリティ施策の残存危険度として、セキュリティの種類各々の残存危険度を前記表示装置に表示すること

を特徴とするセキュリティ評価方法。

【請求項 4】

請求項 1 記載のセキュリティ評価方法であって、

前記データベースは、記述されているセキュリティ施策各々に、そのセキュリティ施策を施すことによって確保されるセキュリティの種類とそのセキュリティ施策を施すのにかかるコストとが併せて記述されており、

前記第 4 のステップは、前記第 2 のステップで読み出した評価対象システムを構成する各機器のセキュリティ施策を、当該セキュリティ施策に対応付けられたセキュリティの種類毎に分類し、セキュリティの種類毎に、当該種類に分類されるセキュリティ施策のうち、前記第 3 のステップで実施有りとされたセキュリテ

ィ施策に対応付けられたコストの総和を求め、これを当該種類に対するセキュリティ施策の所要コストとして、セキュリティの種類各々の所要コストを前記表示装置に表示すること

を特徴とするセキュリティ評価方法。

【請求項5】

請求項1記載のセキュリティ評価方法であって、

前記データベースは、記述されているセキュリティ施策各々に、そのセキュリティ施策を施すことによって確保されるセキュリティのレベルが併せて記述されており、

前記第1のステップは、前記入力装置を介して、操作者より、評価対象システムと当該システムを構成する各機器の指定に加えて、当該システムに施すべきセキュリティ施策のレベルの指定を受け付け、

前記第2のステップは、前記データベースから、前記第1のステップで指定された評価対象システムに対応するシステムタイプの構成機器のうち、前記第1のステップで指定された支援対象システムを構成する各機器に施すべきセキュリティ施策であって、前記第1のステップで指定されたレベル以下のセキュリティ施策を読み出すこと

を特徴とするセキュリティ評価方法。

【請求項6】

請求項1、2、3、4または5記載のセキュリティ評価方法であって、

前記第1のステップは、

前記データベースに記述されているシステムタイプをすべて読み出して前記表示装置に表示し、前記入力装置を介して、操作者より、表示中のシステムタイプのうちのいずれか1つの指定を評価対象システムの指定として受け付けるステップと、

評価対象システムとして指定されたシステムタイプの構成機器すべてを前記データベースから読み出して前記表示装置に表示し、前記入力装置を介して、操作者より、表示中の構成機器各々の評価対象システムでの使用の有無を、評価対象システムを構成する各機器の指定として受け付けるステップと、を有すること

を特徴とするセキュリティ評価方法。

【請求項 7】

電子計算機に、1 以上の機器で構成されるシステムに施されたセキュリティを評価させるためのプログラムが記憶された記憶媒体であって、

前記プログラムは、前記電子計算機に、

当該電子計算機に接続された入力装置を介して、操作者より、評価対象システムと当該システムを構成する各機器の指定を受け付ける第 1 のステップと、

システムタイプ毎に、構成機器と当該構成機器に施すべきセキュリティ施策とが記述されたデータベースを検索し、前記第 1 のステップで指定された評価対象システムに対応するシステムタイプの構成機器のうち、前記第 1 のステップで指定された評価対象システムを構成する各機器に施すべきセキュリティ施策を読み出す第 2 のステップと、

前記第 1 のステップで指定された評価対象システムを構成する機器毎に、前記第 2 のステップで読み出したセキュリティ施策を対応付けて、前記電子計算機に接続された表示装置に表示し、前記入力装置を介して、操作者より、当該機器毎に対応付けて表示されたセキュリティ施策の実施の有無を受け付ける第 3 のステップと、

前記第 3 のステップで受け付けた評価対象システムを構成する各機器のセキュリティ施策の実施の有無に基づいて、当該評価対象システムに施されたセキュリティ状態の評価を行ない、その結果を前記表示装置に表示する第 4 のステップと、
、を実行させること

を特徴とするプログラムが記憶された記憶媒体。

【請求項 8】

1 以上の機器で構成されるシステムに施されたセキュリティを評価するセキュリティ評価装置であって、

システムタイプ毎に、構成機器と当該構成機器に施すべきセキュリティ施策とが記述されたデータベースと、

前記データベースに記述されているシステムタイプをすべて読み出して表示し、操作者より、表示中のシステムタイプのうちのいずれか 1 つの指定を評価対象

システムの指定として受け付ける第 1 の指示受付手段と、

前記第 1 の指示受付手段にて評価対象システムとして指定されたシステムタイプの構成機器すべてを前記データベースから読み出して表示し、操作者より、表示中の構成機器各々の評価対象システムへの使用の有無を、評価対象システムを構成する各機器の指定として受け付ける第 2 の指示受付手段と、

前記第 1 の指示受付手段にて評価対象システムとして指定されたシステムタイプの構成機器のうち、前記第 2 の指示受付手段にて評価対象システムを構成する機器として指定された各構成機器に施すべきセキュリティ施策を、前記データベースから読み出して表示し、操作者より、表示中の各構成機器に施すべきセキュリティ施策の実施の有無を受け付ける第 3 の指示受け手段と、

前記第 3 の指示受け手段で受け付けた各構成機器のセキュリティ施策の実施の有無に基づいて、前記評価対象システムに施されたセキュリティ状態の評価を行ない、その結果を表示する評価手段と、を有すること

を特徴とするセキュリティ評価装置。

【請求項 9】

電子計算機を用いて、1 以上の機器で構成されるシステムに施すべきセキュリティ施策の作成を支援するセキュリティの構築支援方法であって、

前記電子計算機に接続された入力装置を介して、操作者より、支援対象システムと当該システムを構成する各機器の指定を受け付ける第 1 のステップと、

システムタイプ毎に、構成機器と当該構成機器に施すべきセキュリティ施策とが記述されたデータベースを検索し、前記第 1 のステップで指定された支援対象システムに対応するシステムタイプの構成機器のうち、前記第 1 のステップで指定された支援対象システムを構成する各機器に施すべきセキュリティ施策を読み出す第 2 のステップと、

前記第 1 のステップで指定された支援対象システムを構成する機器毎に、前記第 2 のステップで読み出したセキュリティ施策を対応付けて、前記電子計算機に接続された表示装置に表示する第 3 のステップと、を有すること

を特徴とするセキュリティの構築支援方法。

【請求項 10】

請求項 9 記載のセキュリティの構築支援方法であって、

前記データベースは、記述されているセキュリティ施策各々に、そのセキュリティ施策を施すことによって確保されるセキュリティの種類が対応付けられて記述されており、

前記第 2 のステップは、前記データベースから、前記第 1 のステップで指定された支援対象システムに対応するシステムタイプの構成機器のうち、前記第 1 のステップで指定された支援対象システムを構成する各機器に施すべきセキュリティ施策とその種類を読み出し、

前記第 3 のステップは、前記第 1 のステップで指定された支援対象システムを構成する機器毎に、前記第 2 のステップで読み出した支援対象システムを構成する各機器のセキュリティ施策とその種類を対応付けて、前記表示装置に表示すること

を特徴とするセキュリティの構築支援方法。

【請求項 11】

請求項 9 記載のセキュリティの構築支援方法であって、

前記データベースは、記述されているセキュリティ施策各々に、そのセキュリティ施策を施すことによって確保されるセキュリティのレベルが併せて記述されており、

前記第 1 のステップは、前記入力装置を介して、操作者より、支援対象システムと当該システムを構成する各機器の指定に加えて、当該システムに施すべきセキュリティ施策のレベルの指定を受け付け、

前記第 2 のステップは、前記データベースから、前記第 1 のステップで指定された支援対象システムに対応するシステムタイプの構成機器のうち、前記第 1 のステップで指定された支援対象システムを構成する各機器に施すべきセキュリティ施策であって、前記第 1 のステップで指定されたレベル以下のセキュリティ施策を読み出すこと

を特徴とするセキュリティの構築支援方法。

【請求項 1 2】

請求項 9、1 0 または 1 1 記載のセキュリティの構築支援方法であって、
前記第 1 のステップは、

前記データベースに記述されているシステムタイプをすべて読み出して前記表示装置に表示し、前記入力装置を介して、操作者より、表示中のシステムタイプのうちのいずれか 1 つの指定を支援対象システムの指定として受け付けるステップと、

支援対象システムとして指定されたシステムタイプの構成機器すべてを前記データベースから読み出して前記表示装置に表示し、前記入力装置を介して、操作者より、表示中の構成機器各々の支援対象システムでの使用の有無を、支援対象システムを構成する各機器の指定として受け付けるステップと、を有すること
を特徴とするセキュリティの構築支援方法。

【請求項 1 3】

電子計算機に、1 以上の機器で構成されるシステムに施すべきセキュリティ施策の作成を支援させるためのプログラムが記憶された記憶媒体であって、

前記プログラムは、前記電子計算機に、

前記電子計算機に接続された入力装置を介して、操作者より、支援対象システムと当該システムを構成する各機器の指定を受け付ける第 1 のステップと、

システムタイプ毎に、構成機器と当該構成機器に施すべきセキュリティ施策とが記述されたデータベースを検索し、前記第 1 のステップで指定された支援対象システムに対応するシステムタイプの構成機器のうち、前記第 1 のステップで指定された支援対象システムを構成する各機器に施すべきセキュリティ施策を読み出す第 2 のステップと、

前記第 1 のステップで指定された支援対象システムを構成する機器毎に、前記第 2 のステップで読み出したセキュリティ施策を対応付けて、前記電子計算機に接続された表示装置に表示する第 3 のステップと、を実行させること

を特徴とするプログラムが記憶された記憶媒体。

【請求項 1 4】

1 以上の機器で構成されるシステムに施すべきセキュリティ施策の作成を支援

するセキュリティの構築支援装置であって、

システムタイプ毎に、構成機器と当該構成機器に施すべきセキュリティ施策とが記述されたデータベースと、

前記データベースに記述されているシステムタイプをすべて読み出して表示し、操作者より、表示中のシステムタイプのうちのいずれか 1 つの指定を支援対象システムの指定として受け付ける第 1 の指示受付手段と、

前記第 1 の指示受付手段にて支援対象システムとして指定されたシステムタイプの構成機器すべてを前記データベースから読み出して表示し、操作者より、表示中の構成機器各々の支援対象システムでの使用の有無を、支援対象システムを構成する各機器の指定として受け付ける第 2 の指示受付手段と、

前記第 1 の指示受付手段にて支援対象システムとして指定されたシステムタイプの構成機器のうち、前記第 2 の指示受付手段にて支援対象システムを構成する機器として指定された各構成機器に施すべきセキュリティ施策を、前記データベースから読み出し、機器毎に表示するセキュリティ施策表示手段と、を有すること

を特徴とするセキュリティの構築支援装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、1 つ以上の機器で構成されるシステムに対し、当該システムに施されたセキュリティの状態を評価し、あるいは、当該システム固有のセキュリティ施策の作成を支援する技術に関する。

【0002】

【従来の技術】

企業のビジネス活動において、インターネット技術に基づく情報システムが重要なインフラとなってきている。また、企業内情報システムのインターネット接続に対する関心が高まるにつれて、企業内情報システムに対する不正アクセスやウィルスによる情報資産の破壊などのセキュリティ問題が認知されるようになってきている。

【0003】

このようなセキュリティ問題から情報システムを守るため、従来、企業は、個々のセキュリティ問題に対してファイアウォールの設置やウィルス対策ソフトの導入などの個別の技術的対策を行っていた。しかし、近年では、情報システム全体に対する脅威を分析してセキュリティ状態を評価し、その評価結果に基づいて今後の対策方針を作成することにより、対象となる情報システム固有のセキュリティ対策を総合的に実施することが求められるようになりつつある。

【0004】

このような背景から、情報技術製品やこれらの製品で構成された情報システムのセキュリティを体系的に評価・構築するための枠組みとして、セキュリティ評価基準CC (Common Criteria) が1999年6月に国際標準化された (IS 15408)。また、個々の情報システムに施すべきセキュリティポリシーの事例を提示したものとして、米国のセキュリティ専門家であるCharles Cresson Wood氏が作成した運用管理中心のセキュリティポリシー事例集ISPME (Information Security Policy Made Easy) が1997年6月10日にBASELINE software社より出版された。

【0005】

そして、コンサルタントサービスとして、上記のセキュリティ評価基準CCやセキュリティポリシー事例集ISPMEに基づいて、情報システムのセキュリティ状態を評価したり、セキュリティ施策の作成を支援するサービスを提供する者が現れてきている。

【0006】

【発明が解決しようとする課題】

ところで、上記のセキュリティ評価基準CCに基づいて、情報システムのセキュリティ状態を評価したり、セキュリティ施策の作成を支援する場合、体系的に規定されたセキュリティ評価基準CCから、セキュリティ状態の評価対象あるいはセキュリティ施策作成の支援対象となる情報システムを構成する各機器に適用されるべき基準を抽出し、当該情報システムに固有の基準を作成しなければならない。このため、セキュリティ評価基準CCを熟知した、高度な専門知識を有す

るものでなければ実施することができない。したがって、実施に多くの時間がかかり、また、作業コストも高くなる。

【 0 0 0 7 】

また、上記のセキュリティポリシー事例集 I S P M E に基づいて、セキュリティ施策の作成を支援する場合においても、当該事例集 I S P M E のなかからセキュリティ施策作成の支援対象となる情報システムに対応する事例を抽出し、抽出した事例を、当該情報システムの実際の構成に当てはめながら当該情報システムに対するセキュリティポリシーを作成しなければならない。このため、やはり、セキュリティポリシー事例集 I S P M E と情報システムの実際の構成の対応関係を熟知した、高度な専門知識を有するものでなければ実施することができない。したがって、実施に多くの時間がかかり、また、作業コストも高くなる。

【 0 0 0 8 】

本発明は、上記の事情に鑑みてなされたものであり、高度な専門的知識がなくても、システムのセキュリティ状態を評価したり、セキュリティ施策の作成を支援することを可能にすることを目的とする。

【 0 0 0 9 】

【課題を解決するための手段】

上記課題を解決するために、本発明の第 1 の態様は、電子計算機を用いて、1 以上の機器で構成されるシステムに施されたセキュリティを評価するセキュリティ評価方法であって、

前記電子計算機に接続された入力装置を介して、操作者より、評価対象システムと当該システムを構成する各機器の指定を受け付ける第 1 のステップと、

システムタイプ毎に、構成機器と当該構成機器に施すべきセキュリティ施策とが記述されたデータベースを検索し、前記第 1 のステップで指定された評価対象システムに対応するシステムタイプの構成機器のうち、前記第 1 のステップで指定された評価対象システムを構成する各機器に施すべきセキュリティ施策を読み出す第 2 のステップと、

前記第 1 のステップで指定された評価対象システムを構成する機器毎に、前記第 2 のステップで読み出したセキュリティ施策を対応付けて、前記電子計算機に

接続された表示装置に表示し、前記入力装置を介して、操作者より、当該機器毎に対応付けて表示されたセキュリティ施策の実施の有無を、たとえばチェックリスト形式で受け付ける第3のステップと、

前記第3のステップで受け付けた評価対象システムを構成する各機器のセキュリティ施策の実施の有無に基づいて、当該評価対象システムに施されたセキュリティ状態の評価を行ない、その結果を前記表示装置に表示する第4のステップと、を有することを特徴とする。

【0010】

ここで、前記第1のステップは、たとえば、前記データベースに記述されているシステムタイプをすべて読み出して前記表示装置に表示し、前記入力装置を介して、操作者より、表示中のシステムタイプのうちのいずれか1つの指定を評価対象システムの指定として受け付けるステップと、評価対象システムとして指定されたシステムタイプの構成機器すべてを前記データベースから読み出して前記表示装置に表示し、前記入力装置を介して、操作者より、表示中の構成機器各々の評価対象システムでの使用の有無を、評価対象システムを構成する各機器の指定として、たとえばチェックリスト形式で受け付けるステップと、からなるものであってもよい。

【0011】

また、前記データベースに記述されているセキュリティ施策各々に、そのセキュリティ施策を施すことによって確保されるセキュリティの種類が併せて記述されている場合、前記第4のステップは、たとえば、評価対象システムを構成する各機器のセキュリティ施策をセキュリティの種類毎に分類し、セキュリティの種類毎に、当該種類に分類されるセキュリティ施策の数に対する前記第3ステップで実施有りとされたセキュリティ施策の数の割合を求め、これを当該種類に対するセキュリティ施策の達成度として、セキュリティの種類各々の達成度を前記表示装置に表示するようにしてもよい。

【0012】

また、前記データベースに記述されているセキュリティ施策各々に、そのセキュリティ施策を施すことによって確保されるセキュリティの種類とそのセキュリ

ティ施策を施すことによって回避される危険度（この危険度は、たとえば、そのセキュリティ施策を施さなかったことにより発生する可能性のある年間損害額として表わされる）とが併せて記述されている場合、前記第4のステップは、たとえば、評価対象システムを構成する各機器のセキュリティ施策をセキュリティの種類毎に分類し、セキュリティの種類毎に、当該種類に分類されるセキュリティ施策のうち、前記第3ステップで実施無しとされたセキュリティ施策の危険度の総和を求め、これを当該種類に対するセキュリティ施策の残存危険度として、セキュリティの種類各々の残存危険度を前記表示装置に表示するようにしてもよい。

【0013】

あるいは、前記データベースに記述されているセキュリティ施策各々に、そのセキュリティ施策を施すことによって確保されるセキュリティの種類とそのセキュリティ施策を施すのにかかるコスト（このコストは、たとえば、そのセキュリティ施策を施すのにかかる年間コストとして表わされる）とが併せて記述されている場合、前記第4のステップは、たとえば、評価対象システムを構成する各機器のセキュリティ施策をセキュリティの種類毎に分類し、セキュリティの種類毎に、当該種類に分類されるセキュリティ施策のうち、前記第3ステップで実施有りとされたセキュリティ施策のコストの総和を求め、これを当該種類に対するセキュリティ施策の所要コストとして、セキュリティの種類各々の所要コストを前記表示装置に表示するようにしてもよい。

【0014】

本態様では、操作者が、入力装置を用いて、評価対象システムとその構成機器を指定すると、当該評価対象システムを構成する機器毎に、その機器に施すべきセキュリティ施策のリストが表示装置に表示される。操作者は、表示装置に表示された各機器のセキュリティ施策を見て、入力装置を用いて、たとえば表示中のセキュリティ施策にチェックする（いわゆるチェックリスト形式）ことで、その実施の有無を入力することができる。操作者が、入力装置を用いて、表示装置に表示された各機器のセキュリティ施策の実施の有無を入力すると、それに基づいて、評価対象システムに施されたセキュリティ状態の評価を行ない、その結果を表示装置に表示する。

【0015】

このように、本態様によれば、操作者が評価対象システムとその構成機器を指定するだけで、その構成機器各々に施すべきセキュリティ施策が表示される。そして、操作者が表示されている各構成機器のセキュリティ施策の実施の有無を入力するだけで、その評価対象システムに施されているセキュリティの評価を行なうことができる。したがって、操作者は、高度な専門的知識がなくても、システムのセキュリティ状態を評価することが可能となる。

【0016】

次に、上記課題を解決するために、本発明の第2の態様は、電子計算機を用いて、1以上の機器で構成されるシステムに施すべきセキュリティ施策の作成を支援するセキュリティの構築支援方法であって、

前記電子計算機に接続された入力装置を介して、操作者より、支援対象システムと当該システムを構成する各機器の指定を受け付ける第1のステップと、

システムタイプ毎に、構成機器と当該構成機器に施すべきセキュリティ施策とが記述されたデータベースを検索し、前記第1のステップで指定された支援対象システムに対応するシステムタイプの構成機器のうち、前記第1のステップで指定された支援対象システムを構成する各機器に施すべきセキュリティ施策を読み出す第2のステップと、

前記第1のステップで指定された支援対象システムを構成する機器毎に、前記第2のステップで読み出したセキュリティ施策を対応付けて、前記電子計算機に接続された表示装置に、たとえばリスト形式で表示する第3のステップと、を有することを特徴とする。

【0017】

ここで、前記第1のステップは、たとえば、前記データベースに記述されているシステムタイプをすべて読み出して前記表示装置に表示し、前記入力装置を介して、操作者より、表示中のシステムタイプのうちのいずれか1つの指定を支援対象システムの指定として受け付けるステップと、支援対象システムとして指定されたシステムタイプの構成機器すべてを前記データベースから読み出して前記表示装置に表示し、前記入力装置を介して、操作者より、表示中の構成機器各々

の支援対象システムでの使用の有無を、支援対象システムを構成する各機器の指定として、たとえばチェックリスト形式で受け付けるステップと、からなるものであってもよい。

【0018】

また、前記データベースに記述されているセキュリティ施策各々に、そのセキュリティ施策を施すことによって確保されるセキュリティの種類が併せて記述されている場合、前記第2のステップは、前記データベースから、前記第1のステップで指定された支援対象システムに対応するシステムタイプの構成機器のうち、前記第1のステップで指定された支援対象システムを構成する各機器に施すべきセキュリティ施策とその種類を読み出し、前記第3のステップは、前記第1のステップで指定された支援対象システムを構成する機器毎に、前記第2のステップで読み出した支援対象システムを構成する各機器のセキュリティ施策とその種類を対応付けて、前記表示装置に表示するようにしてもよい。

【0019】

また、前記データベースに記述されているセキュリティ施策各々に、そのセキュリティ施策を施すことによって確保されるセキュリティのレベルが併せて記述されている場合、前記第1のステップは、前記入力装置を介して、操作者より、支援対象システムと当該システムを構成する各機器の指定に加えて、当該システムに施すべきセキュリティ施策のレベルの指定を受け付け、前記第2のステップは、前記データベースから、前記第1のステップで指定された支援対象システムに対応するシステムタイプの構成機器のうち、前記第1のステップで指定された支援対象システムを構成する各機器に施すべきセキュリティ施策であって、前記第1のステップで指定されたレベル以下のセキュリティ施策を読み出すようにしてもよい。

【0020】

本態様では、操作者が、入力装置を用いて、支援対象システムとその構成機器を指定すると、当該支援対象システムを構成する機器毎に、その機器に施すべきセキュリティ施策のリストが表示装置に表示される。このように、本態様によれば、操作者が支援対象システムとその構成機器を指定するだけで、その構成機器

各々に施すべきセキュリティ施策が表示されるので、操作者は、高度な専門的知識がなくても、システムに施すべきセキュリティ施策を構築することが可能となる。

【 0 0 2 1 】

【発明の実施の形態】

以下に、本発明の実施の形態について説明する。

【 0 0 2 2 】

まず、本発明の第 1 実施形態について説明する。

【 0 0 2 3 】

図 1 は、本発明の第 1 実施形態が適用されたセキュリティ支援・評価装置 1 の概略構成図である。

【 0 0 2 4 】

図 1 に示すように、本実施形態のセキュリティ支援・評価装置 1 1 は、CPU 1 1 と、メモリ 1 2 と、ハードディスク装置などの外部記憶装置 1 3 と、CD-ROM や FD などの可搬性を有する記憶媒体 1 5 からデータを読み取る読取り装置 1 4 と、キーボードやマウスなどの入力装置 1 6 と、ディスプレイなどの表示装置 1 7 と、ネットワークに接続された通信装置 1 8 と、上述した各構成要素間のデータ送受を司るインターフェース 1 9 とを備えた、一般的な構成を有する電子計算機上に構築することができる。

【 0 0 2 5 】

ここで、外部記憶装置 1 3 には、本実施形態のセキュリティ支援・評価装置 1 1 を電子計算機上に構築するためのセキュリティ評価・構築支援プログラム PG 1 3 2 が格納されており、CPU 1 1 がメモリ 1 2 上にロードされたこのプログラム 1 3 2 を実行することにより、操作者が指定した対象システムの構成機器各々に施すべきセキュリティ施策のリストを作成する施策リスト生成部 1 1 1 と、操作者から受け付けた対象システムの構成機器各々に施すべきセキュリティ施策の実施の有無に基づいて、当該対象システムのセキュリティ状態を評価するセキュリティ評価部 1 1 2 と、入力装置 1 6 や表示装置 1 7 を制御して操作者から各種指示を受け付けたり、施策リスト生成部 1 1 1 やセキュリティ評価部 1 1 2 か

らの出力を表示する入出力制御部 113 とを、プロセスとして実現する。

【0026】

なお、このプログラム 132 は、読取り装置 14 により CD-ROM や FD などの可搬性の記憶媒体 15 から読み取られ、外部記憶装置 13 にインストールされるようにしてもよいし、あるいは、通信装置 18 によりネットワークから外部記憶装置 13 にダウンロードされるようにしてもよい。また、図 1 では、このプログラム 132 を、一旦外部記憶装置 13 に格納してから、メモリ 12 上にロードして CPU 11 により実行するようにしているが、読取り装置 14 により可搬性の記憶媒体 15 から読み取って直接メモリ 12 上にロードし CPU 11 により実行するようにしてもよい。あるいは、通信装置 18 を介してネットワークから直接メモリ 12 上にロードし CPU 11 により実行するようにしてもよい。

【0027】

また、外部記憶装置 13 には、本実施形態によるセキュリティ評価・構築支援の適用が予定されるシステムのタイプ毎に、システムの構成機器各々に適用すべきセキュリティ施策が記述された施策データベース DB₁~DB_n 131 が予め格納されている。本実施形態では、セキュリティ評価・構築支援の適用が予定されるシステムのタイプとして、インターネット接続システム、認証システムおよびプラントシステムを想定している。

【0028】

図 2~図 5 に、施策データベースの一例を示す。

【0029】

ここで、図 2 および図 3 はインターネット接続システムに対応して設けられた施策データベースの内容を示しており、図 4 は認証システムに対応して設けられた施策データベースの内容を示している。そして、図 5 はプラントシステム対応して設けられた施策データベースの内容を示している。

【0030】

図 2~図 5 において、列 201 には、施策種別（セキュリティの種類）が記述される。列 202 には、同じ行の施策種別の欄に記述されたセキュリティを確保するためのセキュリティ施策が記述される。列 203 には、同じ行のセキュリテ

ィ施策の欄に記述されたセキュリティ施策が想定している想定脅威が記述される。列 2 0 4 には、同じ行のセキュリティ施策の欄に記述されたセキュリティ施策について、セキュリティ評価基準 CC (IS 15408) に規定されていれるセキュリティ機能要件 (Security Functional Requirement) のカタログから、その施策を満たす機能要件を選択したものが記述される。列 2 0 5_i には、同じ行のセキュリティ施策の欄に記述されたセキュリティ施策について、それが所定業種（たとえば、金融業など）の基準において実施が義務づけられていればその旨記述される。

【 0 0 3 1 】

また、列 2 0 6_i は、対象システムの構成機器として使用されることが予定される機器毎に設けられ、同じ行のセキュリティ施策の欄に記述されたセキュリティ施策が適用可能である場合に、そのセキュリティ施策を適用することにより確保されるセキュリティのレベル L 1 ~ L 3 と、そのセキュリティ施策を適用するために必要とされる年間の所要コスト C 1 ~ C 5 と、そのセキュリティ施策を適用しなかったことにより同じ行の想定脅威の欄に記述された想定脅威が現実のものとなった場合における年間の損害額を示した残存リスク R 1 ~ R 5 とが記述される。

【 0 0 3 2 】

また、列 2 0 7 は、対象システムの構成機器として使用されることが予定される各機器が設置される施設について、列 2 0 6_i と同様に、同じ行のセキュリティ施策の欄に記述されたセキュリティ施策が適用可能である場合に、そのセキュリティ施策を適用することにより確保されるセキュリティのレベル L 1 ~ L 3 と、そのセキュリティ施策を適用するために必要とされる年間の所要コスト C 1 ~ C 5 と、そのセキュリティ施策を適用しなかったことにより同じ行の想定脅威の欄に記述された想定脅威が現実のものとなった場合における年間の損害額を示した残存リスク R 1 ~ R 5 とが記述される。

【 0 0 3 3 】

そして、列 2 0 8 は、対象システムの運用について、列 2 0 6_i と同様に、同じ行のセキュリティ施策の欄に記述されたセキュリティ施策が適用可能である場

合に、そのセキュリティ施策を適用することにより確保されるセキュリティのレベルL1～L3と、そのセキュリティ施策を適用するために必要とされる年間の所要コストC1～C5と、そのセキュリティ施策を適用しなかったことにより同じ行の想定脅威の欄に記述された想定脅威が現実のものとなった場合における年間の損害額を示した残存リスクR1～R5が記述される。

【0034】

なお、セキュリティのレベルL1～L3、年間の所要コストC1～C5および年間の残存リスクR1～R5の具体的な値は、図2～図5に示すとおりである。

【0035】

たとえば、図2および図3に示すインターネット接続システムに対応して設けられた施策データベースにおいて、セキュリティ施策「個人単位でパスワードを設定」は、施策種別「アクセス権限の管理」に属し、そのセキュリティ施策が想定している想定脅威が「不正使用」であり、また、その施策を満たすセキュリティ機能が、セキュリティ評価基準CC (IS 15408) に規定される機能要件「FMT_MSA. 1」であることを示している。また、このセキュリティ施策「個人単位でパスワードを設定」は、インターネット接続システムの構成機器のうちWWWサーバおよびクライアントに適用可能であることを示している。そして、そのセキュリティ施策をWWWサーバに適用することにより確保されるセキュリティのレベルはL3（最強）であり、そのセキュリティ施策をWWWサーバに適用するために必要とされる年間の所要コストはC2（100万未満）であり、そのセキュリティ施策をWWWサーバに適用しなかったことにより想定脅威「不正使用」が現実のものとなった場合における年間の損害額（残存リスク）はR2（100万未満）であることを示している。また、そのセキュリティ施策をクライアントに適用することにより確保されるセキュリティのレベルはL3（最強）であり、そのセキュリティ施策をクライアントに適用するために必要とされる年間の所要コストはC2（100万未満）であり、そのセキュリティ施策をクライアントに適用しなかったことにより想定脅威「不正使用」が現実のものとなった場合における年間の損害額（残存リスク）はR2（100万未満）であることを示している。

【0036】

なお、図2～図5に示すデータベースの列206_i、207および208の各欄に記入する内容は、事前に行なった脅威分析やリスク分析等の結果に基づいて決定されるようにすることが好ましい。

【0037】

次に、上記構成のセキュリティ支援・評価装置1の動作について説明する。

【0038】

図6および図7は、本発明の第1実施形態であるセキュリティ支援・評価装置1の動作を説明するためのフロー図である。

【0039】

まず、施策リスト生成部111は、入出力制御部113を用いて、表示装置17に、外部記憶装置13に記憶されている施策データベースDB₁～DB_n131の対象システムの名称のリストを含んだ、図8に示すような、セキュリティ施策の作成支援あるいはセキュリティ状態の評価の対象となるシステムの名称を選択するためのGUI画面を表示する（ステップS1001）。

【0040】

図8に示すようなGUI画面を介して、操作者により、入力装置16を使って、セキュリティ施策の作成支援あるいはセキュリティ状態の評価の対象となるシステムの名称が選択（図8ではインターネット接続システムが選択された例を示している）されると（ステップS1002）、施策リスト生成部111は、選択されたシステムの構成機器の名称を外部記憶装置13に記憶されている施策データベースDB₁～DB_n131から読み出す。そして、入出力制御部113を用いて、表示装置17に、選択されたシステムの構成機器の名称のリストを含んだ、図9に示すような、セキュリティ施策の作成支援あるいはセキュリティ状態の評価の対象となるシステムの構成機器の選択するためのGUI画面（図9ではインターネット接続システムを対象システムとした例を示している）を表示する（ステップS1003）。

【0041】

なお、図9において、項目「機器構成」801は、対応する施策データベース

DB₁～DB_n131から読み出された、ステップS1002で選択されたシステムを構成する機器のなかから、セキュリティ施策の作成支援あるいはセキュリティ状態の評価の対象となるシステムに実際に使用されている機器を選択するためのものであり、操作者は入力装置16を使って使用している機器の名称にチェックを入れられるようになっている。項目「環境」802は、対象システムの構成機器が設置される施設や当該対象システムの運用を、セキュリティ施策の作成支援あるいはセキュリティ状態の評価の対象に含めるか否かを設定するためのものであり、操作者は入力装置16を使って含めたいものにチェックを入れられるようになっている。また、項目「セキュリティ強度」803は、セキュリティ施策の作成支援あるいはセキュリティ状態の評価を実施する上でのセキュリティのレベルを設定するためのものであり、操作者は入力装置16を使って設定したいレベルにチェックを入れられるようになっている。ここで、レベル「並」は、対象システムに対し、必要最小限のセキュリティを確保することを目的として、セキュリティ施策の作成支援あるいはセキュリティ状態の評価を実施する場合にチェックすべきレベルであり、図2～図5に示すレベルL1に相当する。レベル「最強」は、最大限のセキュリティを確保することを目的として、セキュリティ施策の作成支援あるいはセキュリティ状態の評価を実施する場合にチェックすべきレベルであり、図2～図5に示すレベルL3に相当する。そして、レベル「強」は、レベル「並」とレベル「最強」の中間に位置するレベルであり、図2～図5に示すレベルL2に相当する。また、ボタン「施策構築支援」804は、本装置1にセキュリティ施策の作成支援を行なわせる場合に選択すべきボタンであり、ボタン「セキュリティ評価」805は、本装置1にセキュリティ評価を行なわせる場合に選択すべきボタンである。

【0042】

さて、図9に示すようなGUI画面を介して、操作者により、入力装置16を使って、必要な項目にチェックが入れられ、ボタン804、805のいずれかが選択されると（ステップS1004）、施策リスト生成部111は、ステップS1002で選択されたシステムに対応する対応する施策データベースDB₁～DB_n131から必要な情報を読み出し、項目「機器構成」801にてチェックさ

れた機器および項目「環境」802にてチェックされた環境毎に、セキュリティ施策リストを作成する（ステップS1005）。

【0043】

以下に、セキュリティ施策リストの作成処理について、図9に示す場合（項目「機器構成」801にてWWWサーバとクライアントがチェックされ、項目「環境」802にて運用がチェックされた場合）を例にとり説明する。

【0044】

まず、図2および図3に示すインターネット接続システムのデータベースの「WWWサーバ」の列206₁の各行において、同じ行のセキュリティ施策が適用可能であり、かつ、当該セキュリティ施策を適用した場合に確保されるセキュリティレベルが、図8の項目「セキュリティ強度」でチェックされたレベル（ここでは「並」=L1）以下のものが記述された行に着目する。そして、着目した各行について、「WWWサーバ」の列206₁に記述された内容と同じ行の列201～204、205₁に記述された内容とを読み出し、これらを基にWWWサーバに対するセキュリティ施策リストを作成する。以上の処理を、「クライアント」の列206₂および「運用」の列208のそれぞれに対しても、同様に実行することで、クライアントに対するセキュリティ施策リストと運用に対するセキュリティ施策リストを作成する。

【0045】

次に、施策リスト生成部111は、図9に示すような画面において、項目「機器構成」801にてチェックされた機器および項目「環境」802にてチェックされた環境毎に、セキュリティ施策リストを作成したならば、ステップS1004で選択されたボタンがボタン「構築支援」804であるか、あるいはボタン「セキュリティ評価」805であるかを判別する（ステップS1006）。

【0046】

選択されたボタンが「構築支援」804である場合、施策リスト生成部111は、入出力制御部113を介して、表示装置17に、ステップS1005で作成した、項目「機器構成」801にてチェックされた機器および項目「環境」802にてチェックされた環境毎のセキュリティ施策リストを表示して、セキュリテ

ィ施策の作成を支援する（ステップS1007）。

【0047】

図10は、セキュリティ施策の作成支援のために表示されるセキュリティ施策リストの一例を示した図である。この例では、図9に示すチェック内容にしたがって、図2および図3に示すインターネット接続システムのデータベースから作成されたリストを示している。ここで、WWWサーバ、クライアントおよび運用各々のセキュリティ施策リストは、別々に表示されるようになっており、操作者は入力装置16を使ってタグ901を選択することにより、所望のセキュリティ施策リストを表示することができる。なお、符号902、903は、現在表示中のセキュリティ施策リストをスクロールさせるためのボタンである。

【0048】

一方、ステップS1006にて、選択されたボタンが「セキュリティ評価」805である場合、セキュリティ評価部112は、入出力制御部113を介して、表示装置17に、ステップS1005で作成した、項目「機器構成」801にてチェックされた機器および項目「環境」802にてチェックされた環境毎のセキュリティ施策リストに含まれるセキュリティ施策各々の実施の有無を確認するためのGUI画面を表示する（ステップS1008）。

【0049】

図11は、セキュリティ評価のために表示されるセキュリティ施策の実施の有無を確認するためのGUI画面の一例を示した図である。この例では、図9に示すチェック内容にしたがって、図2および図3に示すインターネット接続システムのデータベースから作成されたリストに基づいて、GUI画面を作成した例を示している。ここで、図11に示すGUI画面は、図10に示す表示画面に、同じ行に記述されたセキュリティ施策の実施の有無をチェックするための入力欄となる列904が設けられた構成となっている。なお、ボタン「リセット」906は、列906の各入力欄のチェック内容をリセットし、再度チェックし直すためのものである。

【0050】

さて、図11に示すようなGUI画面を介して、操作者により、入力装置16

を使って、各セキュリティ施策の実施の有無がチェックが入れられ、ボタン「実行」905が選択されると（ステップS1009）、セキュリティ評価部112は、入出力制御部113を介して、表示装置17に、図12に示すような、操作者より達成すべきセキュリティの目標レベルを受け付けるためのGUI画面を表示する（ステップS1010）。

【0051】

図12に示す例では、図11に示すGUI画面に表示された機器および環境各々について、セキュリティの目標レベルを、施策種別毎のセキュリティ施策数に対する実施（対策）済のセキュリティ施策数の割合で設定するか（910）、施策種別毎の実施済のセキュリティ施策による所要コストの総額で設定するか（911）、あるいは、施策種別毎の未実施（未対策）のセキュリティ施策による残存リスクの総額で設定するか（912）を、選択することができるようになっている。ここで、セキュリティの目標レベルを施策種別毎のセキュリティ施策数に対する実施済のセキュリティ施策数の割合で設定する場合には、オプションとして特定業界（業界A、B）における基準を適用するか否かを選択できるようになっており、特定業界における基準の適用が選択された場合は、セキュリティの目標レベルが、施策種別毎の当該基準で義務づけられたセキュリティ施策数に対する実施済の当該基準で義務づけられたセキュリティ施策数の割合として設定される。なお、図12では、施策種別毎のセキュリティ施策数に対する実施済のセキュリティ施策数の割合として80%以上が設定された例を示している。

【0052】

さて、図12に示すようなGUI画面を介して、操作者により、入力装置16を使って、セキュリティの目標レベルが設定されると（ステップS1011）、その設定内容にしたがって対象システムのセキュリティ状態を評価する（ステップS1012）。

【0053】

たとえば、ステップS1011において、セキュリティの目標レベルが、施策種別毎のセキュリティ施策数に対する実施済のセキュリティ施策数の割合として設定された場合、セキュリティ評価部112は、図11に示すGUI画面に表示

された機器および環境各々（つまり、WWWサーバ、クライアントおよび運用の各々）について、施策種別毎に、当該種別に分類されるセキュリティ施策数に対する実施済（つまり、実施有無入力欄にチェックが入れられた）セキュリティ施策数の割合を求める（ステップS1013）。そして、入出力制御部113を介して、表示装置17に、その結果であるセキュリティ評価を表示する（ステップS1014）。

【0054】

図13は、セキュリティの目標レベルが施策種別毎のセキュリティ施策数に対する実施済のセキュリティ施策数の割合として設定された場合における、セキュリティ評価結果の表示例を示している。この例では、図12に示すGUI画面において、目標値として80%以上が設定された場合を示している。ここで、WWWサーバ、クライアントおよび運用各々のセキュリティ評価結果は、別々に表示されるようになっており、操作者は入力装置16を使ってタグ913を選択することにより、所望のセキュリティ評価結果を表示することができる。

【0055】

また、図13に示す例では、施策種別毎のセキュリティ施策数に対する実施済のセキュリティ施策数の割合を、各施策種別を軸とする、いわゆるレーダチャートを用いて表示している。ここで、実線は、各軸上における、当該軸が示す施策種別のセキュリティ施策数に対する実施済のセキュリティ施策数の割合に応じた点を結んだ線、すなわちセキュリティ評価結果を示している。一方、一点鎖線は、各軸上における、図12に示すGUI画面で設定された目標値に応じた点を結んだ線である。操作者は、セキュリティ評価結果を示す実線と目標レベルを示す一点鎖線を比較することで、視覚的に、対象システムに施されたセキュリティの状態を把握することが可能となる。

【0056】

なお、ステップS1011において、設定されたセキュリティの目標レベルが、施策種別毎のセキュリティ施策数に対する実施済のセキュリティ施策数の割合であり、かつ、オプションとして特定業界における基準を適用するように設定された場合は、ステップS1013において、図11に示すGUI画面に表示され

た機器および環境各々について、施策種別毎に、当該種別に分類されるセキュリティ施策のうち当該業界基準として義務付けられているセキュリティ施策数に対する実施済の当該業界基準として義務付けられているセキュリティ施策数の割合が求められる。

【 0 0 5 7 】

また、たとえば、ステップ S 1 0 1 1 において、セキュリティの目標レベルが、施策種別毎の実施済のセキュリティ施策による所要コストの総額として設定された場合、セキュリティ評価部 1 1 2 は、図 1 1 に示す G U I 画面に表示された機器および環境各々について、施策種別毎に、当該種別に分類されるセキュリティ施策のうち実施済セキュリティ施策による所要コストの総額を求める（ステップ S 1 0 1 5）。そして、入出力制御部 1 1 3 を介して、表示装置 1 7 に、その結果であるセキュリティ評価を表示する（ステップ S 1 0 1 6）。

【 0 0 5 8 】

図 1 4 は、セキュリティの目標レベルが施策種別毎の実施済のセキュリティ施策による所要コストの総額として設定された場合における、セキュリティ評価結果の表示例を示している。この例では、図 1 2 に示す G U I 画面において、目標値として 1 0 0 万未満／年が設定された場合を示している。また、図 1 4 に示す例では、図 1 3 と同様、施策種別毎の実施済のセキュリティ施策による所要コストの総額を、各施策種別を軸とする、いわゆるレーダチャートを用いて表示している。ここで、実線は、各軸上における、当該軸が示す施策種別の実施済のセキュリティ施策による所要コストの総額に応じた点を結んだ線、すなわちセキュリティ評価結果を示している。一方、一点鎖線は、各軸上における、図 1 2 に示す G U I 画面で設定された目標値に応じた点を結んだ線である。操作者はセキュリティ評価結果を示す実線と目標レベルを示す一点鎖線を比較することで、視覚的に、対象システムに施されたセキュリティの状態を把握することが可能となる。

【 0 0 5 9 】

また、たとえば、ステップ S 1 0 1 1 において、セキュリティの目標レベルが、施策種別毎の未実施のセキュリティ施策による残存リスクの総額として設定された場合、セキュリティ評価部 1 1 2 は、図 1 1 に示す G U I 画面に表示された

機器および環境各々について、施策種別毎に、当該種別に分類されるセキュリティ施策のうち未実施のセキュリティ施策による残存リスクの総額を求める（ステップ S1017）。そして、入出力制御部 113 を介して、表示装置 17 に、その結果であるセキュリティ評価を表示する（ステップ S1018）。

【0060】

図 15 は、セキュリティの目標レベルが施策種別毎の未実施のセキュリティ施策による残存リスクの総額として設定された場合における、セキュリティ評価結果の表示例を示している。この例では、図 12 に示す GUI 画面において、目標値として 100 万未満／年が設定された場合を示している。また、図 15 に示す例では、図 13 と同様、施策種別毎の未実施のセキュリティ施策による残存リスクの総額を、各施策種別を軸とする、いわゆるレーダチャートを用いて表示している。ここで、実線は、各軸上における、当該軸が示す施策種別の未実施のセキュリティ施策による残存リスクの総額に応じた点を結んだ線、すなわちセキュリティ評価結果を示している。一方、一点鎖線は、各軸上における、図 12 に示す GUI 画面で設定された目標値に応じた点を結んだ線である。操作者はセキュリティ評価結果を示す実線と目標レベルを示す一点鎖線を比較することで、視覚的に、対象システムに施されたセキュリティの状態を把握することが可能となる。

【0061】

以上、本発明の第 1 実施形態について説明した。

【0062】

本実施形態では、図 9 に示す GUI 画面において、操作者が、入力装置 16 を用いて、対象システムの構成機器を指定して評価ボタンを選択すると、図 11 に示すような、指定された機器毎にその機器に施すべきセキュリティ施策リストを含んだ GUI 画面が表示装置 17 に表示される。操作者は、表示装置 17 に表示された各機器のセキュリティ施策を見て、入力装置 16 を用いて、実施有無入力欄にチェックする（いわゆるチェックリスト形式）ことで、そのセキュリティ施策の実施の有無を入力することができる。操作者が、入力装置 16 を用いて、表示装置 17 に表示された各機器のセキュリティ施策の実施の有無を入力すると、それに基づいて、対象システムに施されたセキュリティ施策の評価を行ない、そ

の結果を表示装置 1 7 に表示する。

【 0 0 6 3 】

このように、本実施形態によれば、操作者がセキュリティを評価すべき対象システムの構成機器を指定するだけで、その構成機器各々に施すべきセキュリティ施策が表示される。そして、操作者が表示されている各構成機器のセキュリティ施策の実施の有無を入力するだけで、その評価対象システムに施されているセキュリティの評価を行なうことができる。したがって、操作者は、高度な専門的知識がなくても、システムのセキュリティ状態を評価することが可能となる。

【 0 0 6 4 】

また、本実施形態では、図 1 2 に示す G U I 画面において、操作者はセキュリティの目標レベルを設定することができる。また、図 1 3 ～図 1 5 に示すように、セキュリティ評価結果は、設定した目標レベルと対比できるようにして表示される。このため、操作者は、評価対象システムの規模や評価対象システムに要求されるセキュリティレベルなどの、当該評価対象システムに固有の事情が考慮されたセキュリティ評価結果を得ることができる。

【 0 0 6 5 】

また、本実施形態では、図 9 に示す G U I 画面において、操作者が、入力装置 1 6 を用いて、対象システムの構成機器を指定して構築支援ボタンを選択すると、図 1 0 に示すような、指定された機器毎にその機器に施すべきセキュリティ施策リストを含んだ G U I 画面が表示装置 1 7 に表示される。このように本実施形態によれば、操作者がセキュリティ施策を構築すべき対象システムの構成機器を指定するだけで、その構成機器各々に施すべきセキュリティ施策が表示されるので、操作者は、高度な専門的知識がなくても、システムに施すべきセキュリティ施策を構築することが可能となる。

【 0 0 6 6 】

また、図 9 に示す G U I 画面において選択されたセキュリティ強度以下のセキュリティ施策が図 1 0 に示すセキュリティ施策リストに表示されるので、操作者は、対象システムの規模や対象システムに要求されるセキュリティレベルなどの、当該対象システムに固有の事情が考慮して、当該システムに施すべきセキュリ

ティ施策のリストを表示させることができる。

【0067】

次に、本発明の第2実施形態について説明する。

【0068】

図16は、本発明の第2実施形態が適用されたセキュリティ支援・評価システムの概略図である。

【0069】

上記の第1実施形態では、セキュリティ施策データベース $DB_1 \sim DB_n$ 131を、セキュリティ支援・評価装置1の外部記憶装置13に格納した場合について説明した。これに対し、本実施形態では、図16に示すように、セキュリティ支援・評価装置1がたとえば携帯型の電子計算機上に構築される場合を考慮し、セキュリティ施策データベース $DB_1 \sim DB_n$ 131をセキュリティ支援・評価装置1とは別の電子計算機上に構築されたデータベース管理装置 $2_1 \sim 2_n$ ($n \geq 1$)に格納し、セキュリティ支援・評価装置1は、公衆網などのネットワークを介してデータベース管理装置 2_i ($1 \leq i \leq n$)にアクセスし、セキュリティ施策リスト作成に必要な情報を得るようにしている。

【0070】

図17は、本発明の第2実施形態に用いるセキュリティ支援・評価装置1の概略構成図である。ここで、図1に示す第1実施形態のセキュリティ支援・評価装置1と同じ機能を有するものには同じ符号を付している。

【0071】

図示するように、本実施形態のセキュリティ支援・評価装置1が、図1に示す第1実施形態のセキュリティ支援・評価装置1と異なる点は、外部記憶装置13にセキュリティ施策データベース $DB_1 \sim DB_n$ 131が格納されていない点と、外部記憶装置13に、ネットワークを介してデータベース管理装置 $2_1 \sim 2_n$ にアクセスするための通信プログラムPG133、および、図18に示すようなデータベース管理装置 $2_1 \sim 2_n$ の各々アクセス先（アドレス）が記述されたDBアドレス管理テーブル134が格納されている点である。CPU11は、通信プログラム133をメモリ12上にロードし実行することで、通信部18により公衆網

などのネットワークを介してデータベース管理装置 $2_1 \sim 2_n$ にアクセスし、データベース管理装置 $2_1 \sim 2_n$ の間の通信を実現するために必要な各種プロトコル群を処理する通信制御部 1 1 4 をプロセスとして実現する。

【0072】

図 1 9 は、本発明の第 2 実施形態に用いるデータベース管理装置 2_i ($1 \leq i \leq n$) の概略構成図である。ここで、図 1 に示す第 1 実施形態のセキュリティ支援・評価装置 1 と同じ機能を有するものには同じ符号を付している。

【0073】

図示するように、本実施形態のデータベース管理装置 2_i は、図 1 7 に示すセキュリティ支援・評価装置 1 と異なる点は、外部記憶装置 1 3 に、DB アドレス管理テーブル 1 3 4 および評価・構築支援プログラム PG 1 3 2 に代えて、セキュリティ施策データベース DB_i 1 3 1 および DB 管理プログラム PG 1 3 5 が格納されている点である。CPU 1 1 は、DB 管理プログラム 1 3 5 をメモリ 1 2 上にロードし実行することで、通信制御部 1 1 4 を介して、セキュリティ支援・評価装置 1 より受け取った要求に応じて、外部記憶装置 1 3 に格納されているセキュリティ施策データベース DB_i 1 3 1 から必要な情報を読み出し、セキュリティ支援・評価装置 1 に送信するデータベース DB 検索部 1 1 5 をプロセスとして実現する。

【0074】

次に、上記構成のセキュリティ支援・評価システムの動作について説明する。

【0075】

まず、図 1 7 に示すセキュリティ支援・評価装置 1 の動作について説明する。

【0076】

本実施形態のセキュリティ支援・評価装置 1 の動作は、図 6 および図 7 に示す第 1 実施形態のセキュリティ支援・評価装置 1 の動作と基本的に同様である。ただし、以下の点で異なる。

【0077】

すなわち、ステップ S 1 0 0 1 において、セキュリティ支援・評価装置 1 は、データベース管理装置 $2_1 \sim 2_n$ が格納するセキュリティ施策データベース DB₁

～DB_n131 各々の対象システムの名称を、予め外部記憶装置 13 などに記憶しており、施策リスト生成部 111 は、外部記憶装置 13 からセキュリティ施策データベース DB₁～DB_n131 の対象システム各々の名称を読み出し、入出力制御部 113 を用いて、図 8 に示すような GUI 画面を表示する。

【0078】

また、ステップ S1003 において、施策リスト生成部 111 は、ステップ S1002 で選択されたシステムのセキュリティ施策データベースを格納するデータベース管理装置 2_i より当該システムの構成機器の名称を読み出すため指示を通信制御部 114 に渡す。これを受けて、通信制御部 114 は、当該データベース管理装置 2_i のアドレスを外部記憶装置 13 に格納されている DB アドレス管理テーブル 134 から取得し、通信装置 18 を介して、当該データベース管理装置 2_i に指示を送信する。その後、通信制御部 114 は、当該データベース管理装置 2_i から当該システムの構成機器の名称が送られてくると、これらを施策リスト生成部 111 に渡す。これを受けて、施策リスト生成部 111 は、入出力制御部 113 を用いて、受け取った構成機器の名称のリストを含んだ、図 9 に示すような GUI 画面を表示する。

【0079】

さらに、ステップ S1005 において、図 20 に示す処理を行なう。

【0080】

まず、施策リスト生成部 111 は、ステップ S1002 で選択されたシステムのセキュリティ施策データベースを格納するデータベース管理装置 2_i より必要な情報を読み出すための検索指示を、ステップ S1004 にて図 9 に示すような GUI 画面を介して操作者によりチェックされた項目の内容とともに、通信制御部 114 に渡す（ステップ S1101）。

【0081】

これを受けて、通信制御部 114 は、当該データベース管理装置 2_i のアドレスを外部記憶装置 13 に格納されている DB アドレス管理テーブル 134 から取得し、通信装置 18 を介して、当該データベース管理装置 2_i に、前記チェックされた項目の内容を含んだデータベースの検索指示を送信する（ステップ S11

02)。その後、通信制御部114は、当該データベース管理装置2_iから検索結果が送られてくると（ステップS1103）、これらを施策リスト生成部111に渡す。

【0082】

これを受けて、施策リスト生成部111は、検索結果に基づいて、図9に示すGUI画面の項目「機器構成」801にてチェックされた機器および項目「環境」802にてチェックされた環境毎に、セキュリティ施策リストを作成する（ステップS1104）。

【0083】

次に、図19に示すデータベース管理装置2_iの動作について説明する。

【0084】

図21は、本発明の第2実施形態で用いるデータベース管理装置2_iの動作を説明するためのフロー図である。

【0085】

まず、通信制御部114は、通信装置18を介して、セキュリティ支援・評価装置1からシステムの構成機器の名称を読み出すため指示を受け取ると（ステップS2001）、これをDB検索部115に渡す。これを受けて、DB検索部115は、外部記憶装置13に格納されているセキュリティ施策データベースDB_iから、当該データベースの列206に記述されている各構成機器の名称を読み出し（図2～図5参照）、通信制御部114に渡す（ステップS2002）。通信制御部114は、受け取った各構成機器の名称を、セキュリティ支援・評価装置1に送信する（ステップS2003）。

【0086】

次に、通信制御部114は、通信装置18を介して、セキュリティ支援・評価装置1から、図9に示すGUI画面でチェックされた構成機器や環境の名称およびセキュリティ強度を含んだ検索指示を受け取ると（ステップS2004）、これをDB検索部115に渡す。これを受けて、DB検索部115は、外部記憶装置13に格納されているセキュリティ施策データベースDB_iから必要な情報を読み出す（ステップS2005）。

【 0 0 8 7 】

たとえば、外部記憶装置 1 3 に格納されているセキュリティ施策データベース DB₁ が図 2 および図 3 に示すインターネット接続システムのものであり、検索指示に含まれる構成機器および環境の名称が、「WWWサーバ」、「クライアント」および「運用」であり、セキュリティ強度が「並」である場合、以下のようにして必要な情報を読み出す。

【 0 0 8 8 】

まず、図 2 および図 3 に示すインターネット接続システムのデータベースの「WWWサーバ」の列 2 0 6₁ の各行において、同じ行のセキュリティ施策が適用可能であり、かつ、当該セキュリティ施策を適用した場合に確保されるセキュリティレベルが、検索指示に含まれるセキュリティ強度（ここでは「並」= L 1）以下のものが記述された行に着目する。そして、着目した各行について、「WWWサーバ」の列 2 0 6₁ に記述された内容と同じ行の列 2 0 1 ~ 2 0 4、2 0 5₁ に記述された内容とを読み出す。以上の処理を、「クライアント」の列 2 0 6₂ および「運用」の列 2 0 8 のそれぞれに対しても、同様に実行することで、検索指示に含まれる構成機器および環境毎に、必要な情報を読み出す。

【 0 0 8 9 】

次に、DB 検索部 1 1 5 は、上記のようにして読み出した情報を通信制御部 1 1 4 に渡す。通信制御部 1 1 4 は、受け取った情報を、検索結果として、セキュリティ支援・評価装置 1 に送信する（ステップ S 2 0 0 6）。

【 0 0 9 0 】

以上、本発明の第 2 実施形態について説明した。

【 0 0 9 1 】

本実施形態では、セキュリティ施策データベース DB₁ ~ DB_n 1 3 1 をセキュリティ支援・評価装置 1 とは別の電子計算機上に構築されたデータベース管理装置 2₁ ~ 2_n に格納し、セキュリティ支援・評価装置 1 は、公衆網などのネットワークを介してデータベース管理装置 2₁ にアクセスし、セキュリティ施策リスト作成に必要な情報を得るようにしているので、セキュリティ支援・評価装置 1 を、たとえば携帯型の電子計算機上に構築する場合に好適である。

【0092】

なお、上記の実施形態において、セキュリティ支援・評価装置1は、データベース管理装置 $2_1 \sim 2_n$ が格納するセキュリティ施策データベース $DB_1 \sim DB_n$ 131各々の対象システムの名称を、予め外部記憶装置13などに記憶しておくようにしているが、この情報は、セキュリティ支援・評価装置1がデータベース管理装置 $2_1 \sim 2_n$ 各々に定期的にアクセスすることで、取得するようにしてもよい。また、この際、各データベース管理装置 $2_1 \sim 2_n$ から、セキュリティ施策データベースの対象システムの名称とともに当該対象システムの構成機器の名称も併せて取得しておくようにすれば、上述した図6のステップS1003の変更は不要になる。

【0093】

【発明の効果】

以上説明したように、本発明によれば、高度な専門的知識がなくても、システムのセキュリティ状態を評価したり、セキュリティ施策の作成を支援することが可能になる。

【図面の簡単な説明】

【図1】

本発明の第1実施形態が適用されたセキュリティ支援・評価装置1の概略構成図である。

【図2】

インターネット接続システムに対応するセキュリティ施策データベースの一例を示す図である。

【図3】

インターネット接続システムに対応するセキュリティ施策データベースの一例を示す図である。

【図4】

認証システムに対応するセキュリティ施策データベースの一例を示す図である。

【図 5】

プラントシステムに対応するセキュリティ施策データベースの一例を示す図である。

【図 6】

本発明の第 1 実施形態であるセキュリティ支援・評価装置 1 の動作を説明するためのフロー図である。

【図 7】

本発明の第 1 実施形態であるセキュリティ支援・評価装置 1 の動作を説明するためのフロー図である。

【図 8】

セキュリティ施策の作成支援あるいはセキュリティ状態の評価の対象となるシステムの名称を選択するための G U I 画面の例を示した図である。

【図 9】

セキュリティ施策の作成支援あるいはセキュリティ状態の評価の対象となるシステムの構成機器の選択するための G U I 画面の例を示した図である。

【図 1 0】

セキュリティ施策の作成支援のために表示されるセキュリティ施策リストの一例を示した図である。

【図 1 1】

セキュリティ評価のために表示されるセキュリティ施策の実施の有無を確認するための G U I 画面の一例を示した図である。

【図 1 2】

操作者より達成すべきセキュリティの目標レベルを受け付けるための G U I 画面の例を示した図である。

【図 1 3】

セキュリティの目標レベルが施策種別毎のセキュリティ施策数に対する実施済のセキュリティ施策数の割合として設定された場合における、セキュリティ評価結果の表示例を示す図である。

【図 1 4】

セキュリティの目標レベルが施策種別毎の実施済のセキュリティ施策による所要コストの総額として設定された場合における、セキュリティ評価結果の表示例を示す図である。

【図 1 5】

セキュリティの目標レベルが施策種別毎の未実施のセキュリティ施策による残存リスクの総額として設定された場合における、セキュリティ評価結果の表示例を示す図である。

【図 1 6】

本発明の第 2 実施形態が適用されたセキュリティ支援・評価システムの概略図である。

【図 1 7】

本発明の第 2 実施形態に用いるセキュリティ支援・評価装置 1 の概略構成図である。

【図 1 8】

本発明の第 2 実施形態に用いるセキュリティ支援・評価装置 1 の外部記憶装置 1 3 に格納されている DB アドレス管理テーブル 1 3 4 を説明するための図である。

【図 1 9】

本発明の第 2 実施形態に用いるデータベース管理装置 2_i ($1 \leq i \leq n$) の概略構成図である。

【図 2 0】

本発明の第 2 実施形態に用いるセキュリティ支援・評価装置 1 における、図 6 のステップ S 1 0 0 5 の処理を説明するためのフロー図である。

【図 2 1】

本発明の第 2 実施形態で用いるデータベース管理装置 2_i の動作を説明するためのフロー図である。

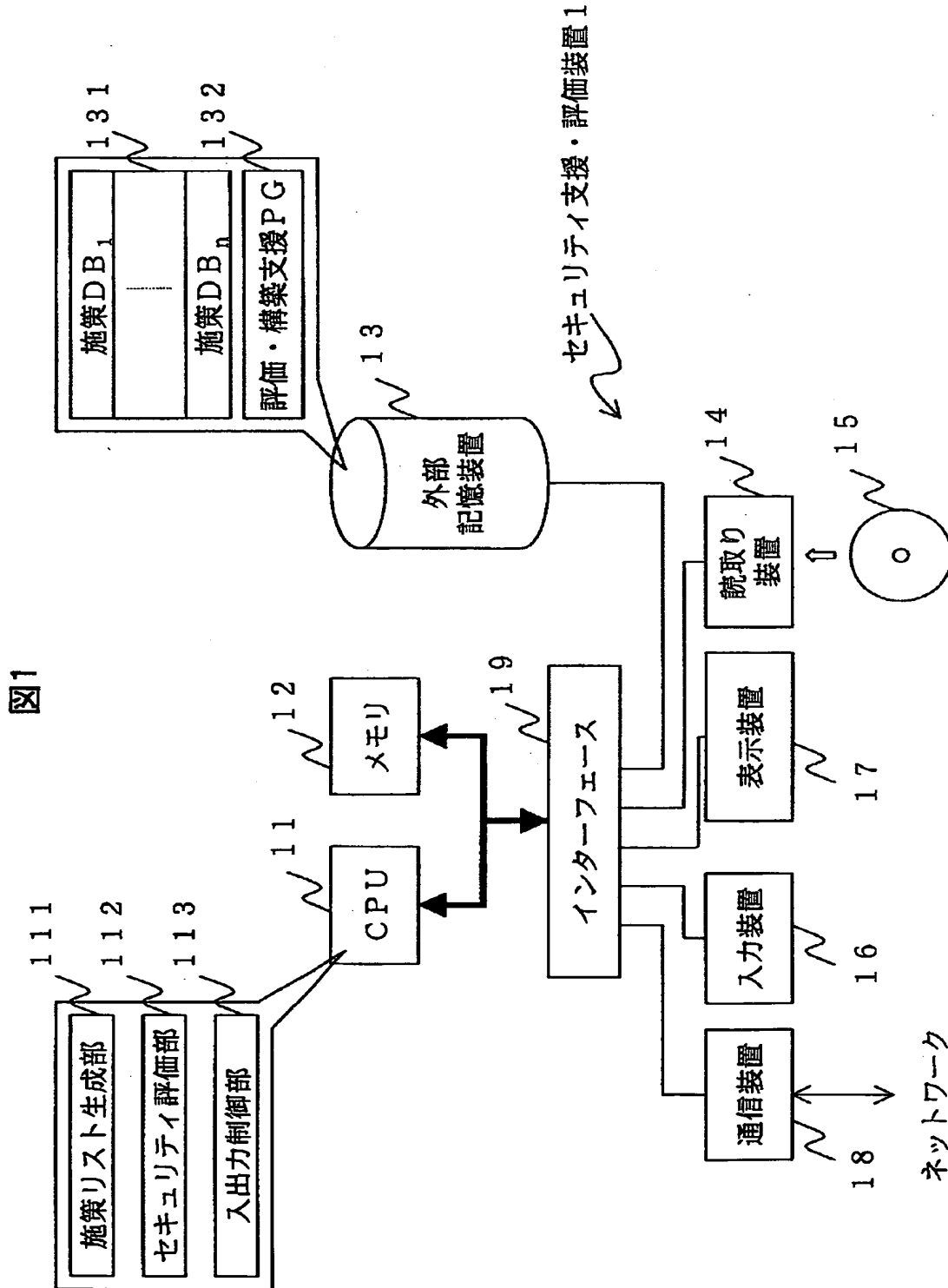
【符号の説明】

1・・・セキュリティ支援・評価装置

- 2₁~2_n…データベース管理装置
- 11…CPU
- 12…メモリ
- 13…外部記憶装置
- 14…読取り装置
- 15…過般性のある記憶媒体
- 16…入力装置
- 17…表示装置
- 18…通信装置
- 19…インターフェース
- 111…施策リスト生成部
- 112…セキュリティ評価部
- 113…入出力制御部
- 114…通信制御部
- 115…DB検索部
- 131…セキュリティ施策データベースDB₁~DB_n
- 132…評価・構築支援プログラムPG
- 133…通信プログラムPG
- 134…データベースアドレステーブル
- 135…データベース管理プログラムPG

【書類名】 図面

【図 1】



【図 2】

インターネット接続システム (その1)

図2

201	202	203	204	205	206	206 ₁	206 ₂	206 ₃	207	208
施策種別	セキュリティ施策	想定脅威	CC機能要件	業種A基準	業種B基準	WWWサーバ	クライアント	ポータルータ	施設	運用
アクセス権限の管理	アクセス権限の管理者を設定	不正使用		◎	◎					L2, C2, R4
アクセス権限の管理	個人単位でパスワードを設定	不正使用	FMT_MSA.1			L3, C2, R2	L3, C2, R2			
アクセス権限の管理	アクセス権限の設定状況を随時確認可能に設定	不正使用	FMT_MSA.1 FMT_MTD.1			L2, C2, R3	L2, C2, R3			
アクセス権限の管理	アクセスを特権ユーザに限定	情報漏洩	FDP_ACF.1 FDP_ACF.2 FIA_UID.1	◎		L1, C2, R3	L3, C1, R3			
アクセス権限の管理	管理ユーティリティの利用可能者を限定	情報漏洩	FDP_ACC.1 FDP_ACF.1			L1, C1, R3	L1, C1, R3	L1, C1, R3		
.....
識別と認証	リモートアクセスで特権ユーザになれる端末限定	不正使用	FIA_UAU.2 FIA_UID.1	◎		L3, C3, R3		L2, C4, R3		
識別と認証	IPアドレスで相手を確認	不正使用				L2, C2, R3		L1, C2, R3		
識別と認証	認証失敗時に各種情報を表示せず	不正使用	FIA_AFL.1 FIA_UAU.7			L1, C1, R2	L1, C2, R2	L1, C2, R2		
識別と認証	1回の認証失敗でユーザIDをロック	不正使用	FIA_AFL.1			L2, C3, R3		L1, C3, R3		
.....

セキュリティレベル
L1: 並, L2: 強, L3: 最強

年間所要コスト

C1: 10万未満, C2: 100万未満, C3: 500万未満,
C4: 1000万未満, C5: 1000万以上

年間残存リスク

R1: 10万未満, R2: 100万未満, R3: 500万未満,
R4: 1000万未満, R5: 1000万以上

インターネット接続システム (その2)

図3

【図 3】

201 202 203 204 205 206 206₁ 206₂ 206₃ 207 208

施策種別	セキュリティ施策	想定脅威	CC機能要件	業種A基準	業種B基準	WWWサーバ	クライアント	ポータル	施設	運用
ウイルス対策	ウイルスチェックを定期的に起動	情報改竄				L3, C2, R3	L1, C1, R3			
ウイルス対策	ウイルス定義を定期的に更新	情報改竄				L3, C2, R3	L1, C1, R2			
ウイルス対策	FD等の可搬性記憶媒体を使用不可に設定	情報改竄				L3, C1, R2	L3, C1, R2			
ウイルス対策	デーモン起動機構を定期的にチェック	情報改竄				L3, C3, R3				
ウイルス対策	不要なサービスを停止	不正使用				L2, C2, R3	L1, C2, R3			
.....
入退室管理	出入り口に施錠	機器破壊		◎					L1, C4, R4	
入退室管理	入室に必要な鍵等を所定場所に管理・管理	機器破壊								L2, C2, R4
入退室管理	入室許可証を発行	機器破壊								L2, C2, R4
入退室管理	入室管理にレベルを設定	機器破壊								L3, C3, R4
.....

セキュリティレベル
L1: 並, L2: 強, L3: 最強

年間所要コスト

C1: 10万未満, C2: 100万未満, C3: 500万未満,
C4: 1000万未満, C5: 1000万以上

年間残存リスク

R1: 10万未満, R2: 100万未満, R3: 500万未満
R4: 1000万未満, R5: 1000万以上

【図 4】

図4

認証システム

201	202	203	204	205	206	206 ₂	206 ₃	207	208	
施策種別	セキュリティ施策	想定脅威	CC機能要件	業種A基準	業種B基準	認証サーバ	暗号装置	ルータ	施設	運用
認証書管理	認証書の有効期限を設定	不正使用	FMT_SAB.1 FMT_MSA.1			L1, C3, R4				
認証書管理	認証書を無効にする前に本人の識別・認証を実行	不正使用	FIA_UID.2 FIA_UAU.1			L2, C3, R4	L1, C3, R4			
.....
鍵管理	不許可になった鍵へのアクセスを監査証跡に記録	不正使用	PAU_GEN.1 PAU_SAR.1 PAU_SAR.3			L2, C3, R5	L1, C3, R5	L3, C3, R5		
.....
侵入者対策	外部ネットワークとの接続点にファイアウォール	情報漏洩							L1, C4, R5	
.....
入退室管理	資格変更に伴う許可証の変更・回収を迅速に	機器破壊								L2, C4, R5
.....

セキュリティレベル
L1: 並, L2: 強, L3: 最強

年間所要コスト
C1: 10万未満, C2: 100万未満, C3: 500万未満,
C4: 1000万未満, C5: 1000万以上

年間残存リスク
R1: 10万未満, R2: 100万未満, R3: 500万未満,
R4: 1000万未満, R5: 1000万以上

【図 5】

図5

プラントシステム

201	202	203	204	205	206	206 ₁	206 ₂	206 ₃	207	208
施策種別	セキュリティ施策	想定脅威	CC機能要件	業種A基準	業種B基準	制御装置	管理装置	ファイアウォール	施設	運用
プラント操作権限管理	操作前に、本人の識別・認証を実行	不正使用	FIA_UID.2 FMT_UAU.1			L2, C3, R4	L1, C3, R4	L1, C3, R4		
プラント操作権限管理	技術レベルを考慮してユーザに特権を付与	不正使用	FMT_MSA.1							L1, C3, R4
.....
プラント操作監視	不許可になった操作を監査証跡に記録	不正使用	FAU_GEN.1 FAU_SAR.1 FAU_SAR.3			L2, C3, R5	L1, C3, R5	L3, C3, R5		
.....
侵入者対策	外部ネットワークとの接続点にファイアウォール	情報漏洩							L1, C4, R5	
.....
入退室管理	入室管理にレベルを設定	機器破壊								L2, C4, R5
.....

セキュリティレベル

L1:並, L2:強, L3:最強

年間所要コスト

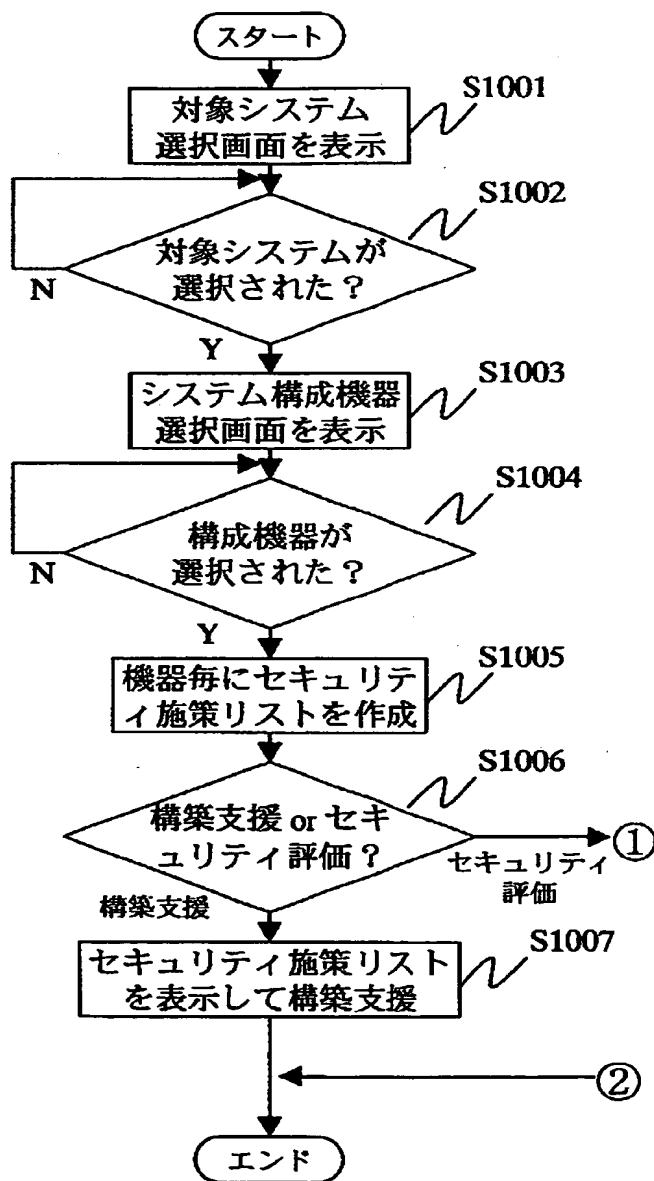
C1:10万未満, C2:100万未満, C3:500万未満,
C4:1000万未満, C5:1000万以上

年間残存リスク

R1:10万未満, R2:100万未満, R3:500万未満,
R4:1000万未満, R5:1000万以上

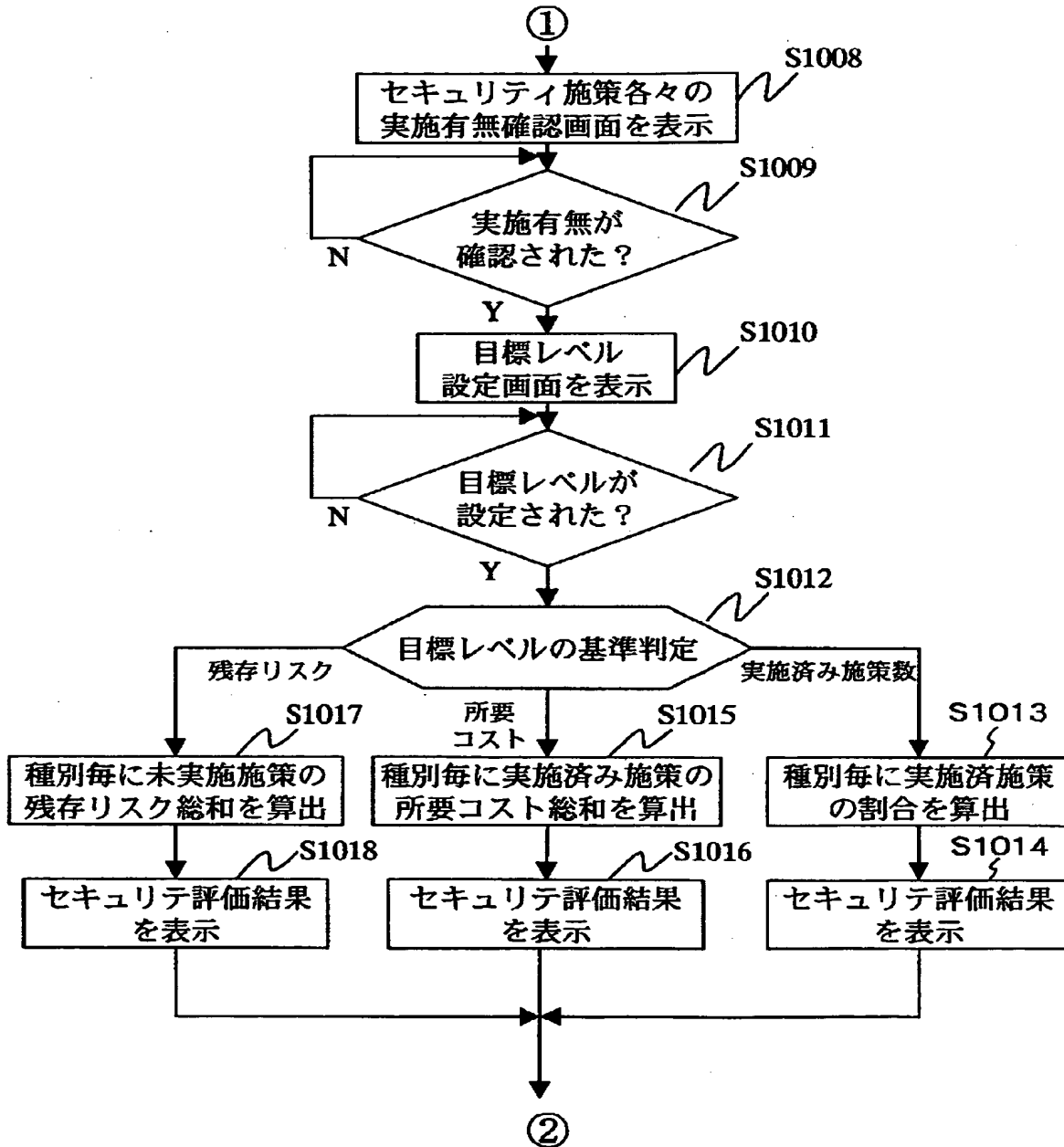
【図 6】

図 6



【図 7】

図 7



【図 8】

図 8

対象システム

☒ インターネット接続システム

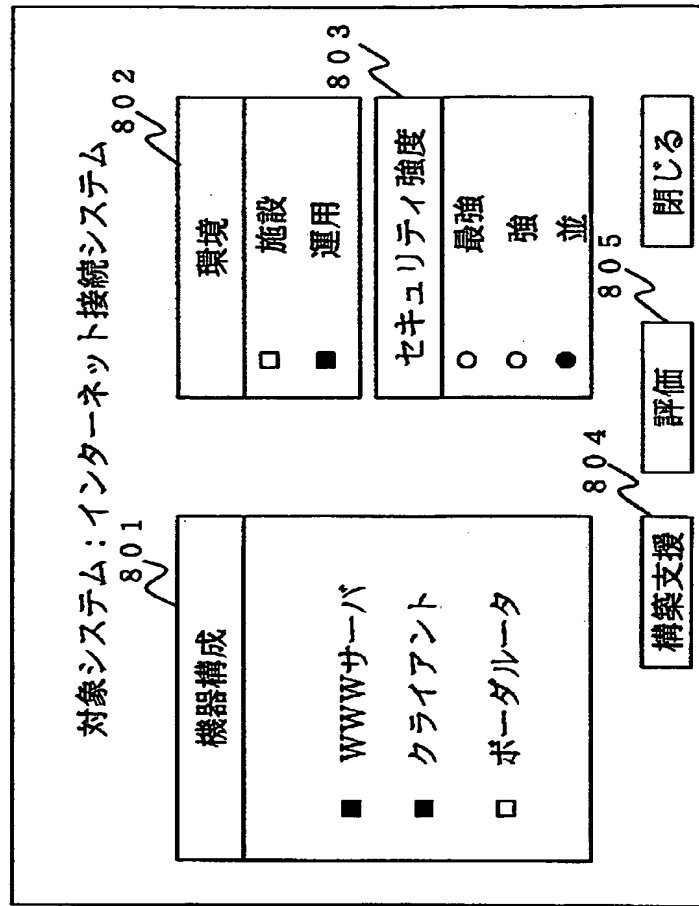
☐ 認証システム

☐ プラントシステム

OK 閉じる

【図 9】

図 9



【図 1 0】

図 1 0

901

対象システム：インターネット接続システム

902

903

施策種別	セキュリティ施策	想定脅威	CC機能要件	業種A基準	業種B基準	所要コスト	残存リスク
アクセス権限の管理	アクセスを特権ユーザに限定	情報漏洩	FDP_ACR.1 FDP_ACC.2 FIA_UAU.1	◎		100万未満	500万未満
アクセス権限の管理	管理ユーザの利用可能者を限定	情報漏洩	FDP_ACR.1 FDP_ACC.1 FDP_ACR.1			10万未満	500万未満
.....
識別と認証	認証失敗時に各種情報を表示せず	不正使用	FIA_APL.1 FIA_UAU.7			10万未満	500万未満
.....

保存印刷閉じる

【図 1 1】

図 1 1

901 対象システム：インターネット接続システム

904

WWWサーバ		クライアント		運用							
施策種別	セキュリティ施策	想定脅威	CC機能要件	業種A基準	業種B基準	所要コスト	残存リスク	有無入力欄			
アクセス権限の管理	アクセスを特権ユーザに限定	情報漏洩	FDP_ACF.1 FDP_ACC.1 FIA_UAU.1	◎		100万未満	500万未満	✓			
アクセス権限の管理	管理ユーティリティの利用可能者を限定	情報漏洩	FDP_ACC.1 FDP_ACF.1			10万未満	500万未満	✓			
.....			
識別と認証	認証失敗時に各種情報を表示せず	不正使用	FIA_AFL.1 FIA_UAU.7			10万未満	500万未満	✓			
.....			

905

実行

906

リセット

閉じる

【図 1 2】

図 1 2

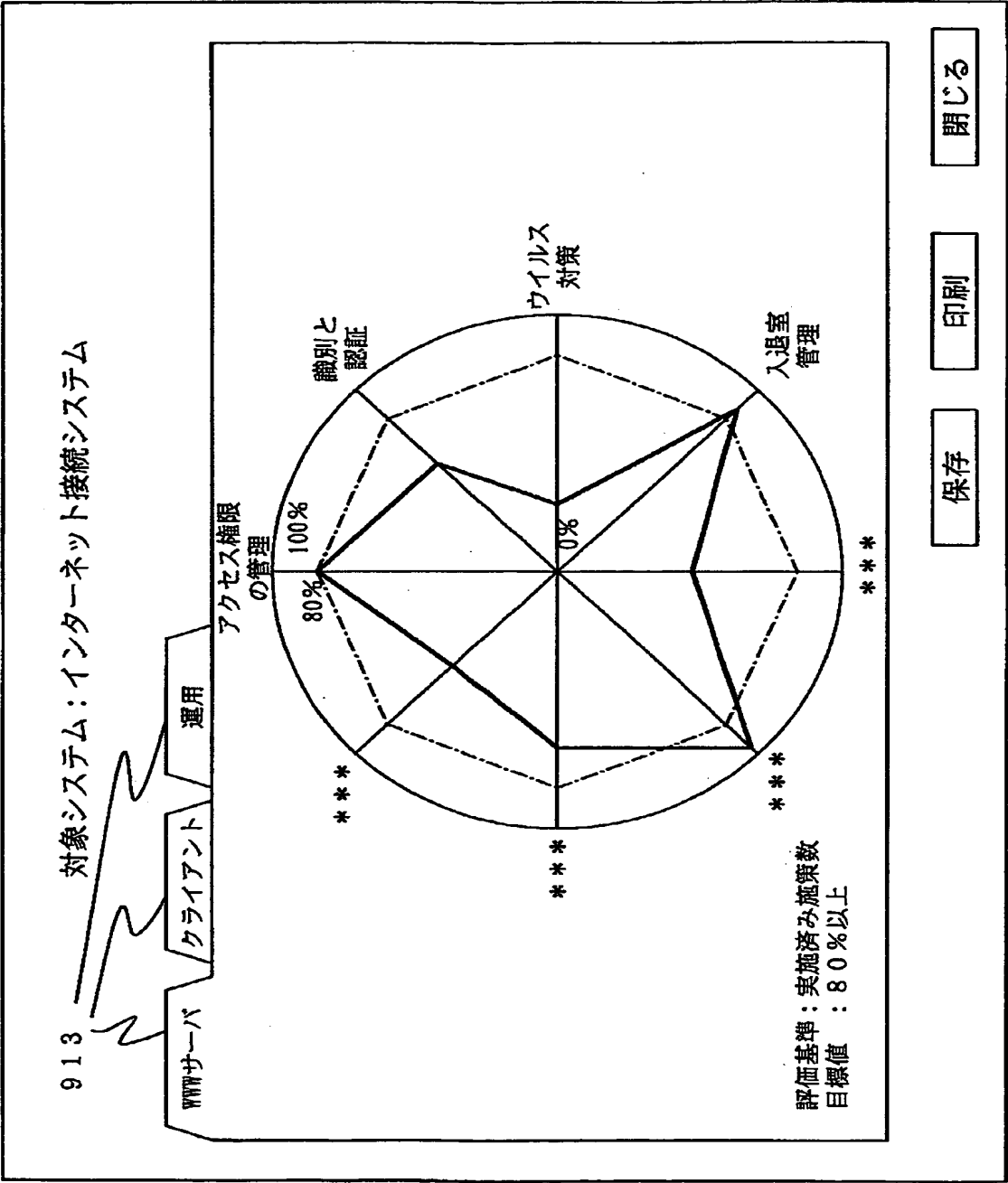
目標レベル設定

<input checked="" type="radio"/> 対策済みセキュリティ施策数 目標値 <input style="width: 50px; text-align: center;" type="text" value="80"/> %以上	<input type="radio"/> 業界A基準 <input type="radio"/> 業界B基準
<input type="radio"/> 所要コスト 目標値 <input style="width: 50px;" type="text"/> 万未満/年	
<input type="radio"/> 残存リスク 目標値 <input style="width: 50px;" type="text"/> 万未満/年	

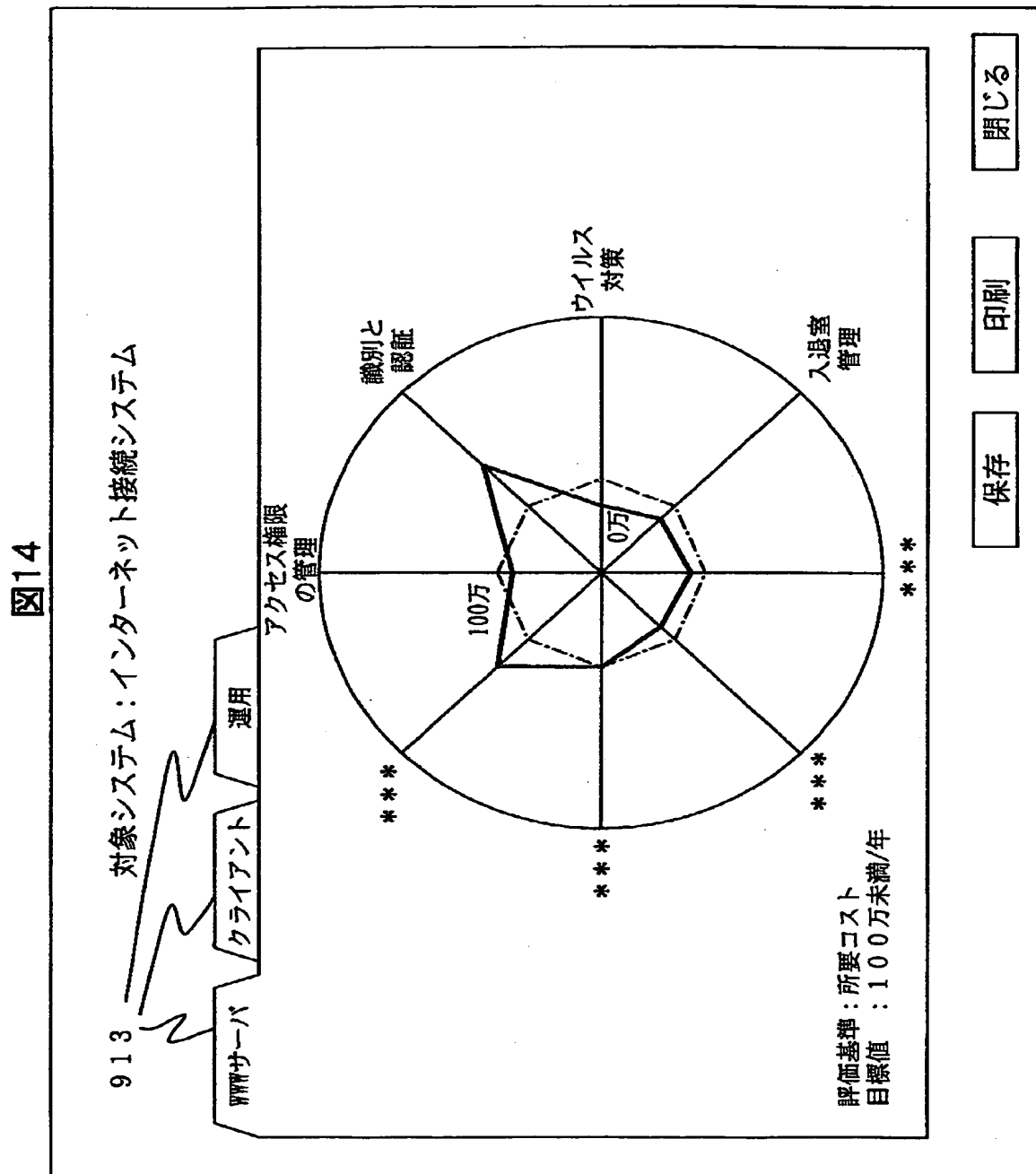
9 1 0
 9 1 1
 9 1 2

【図 1 3】

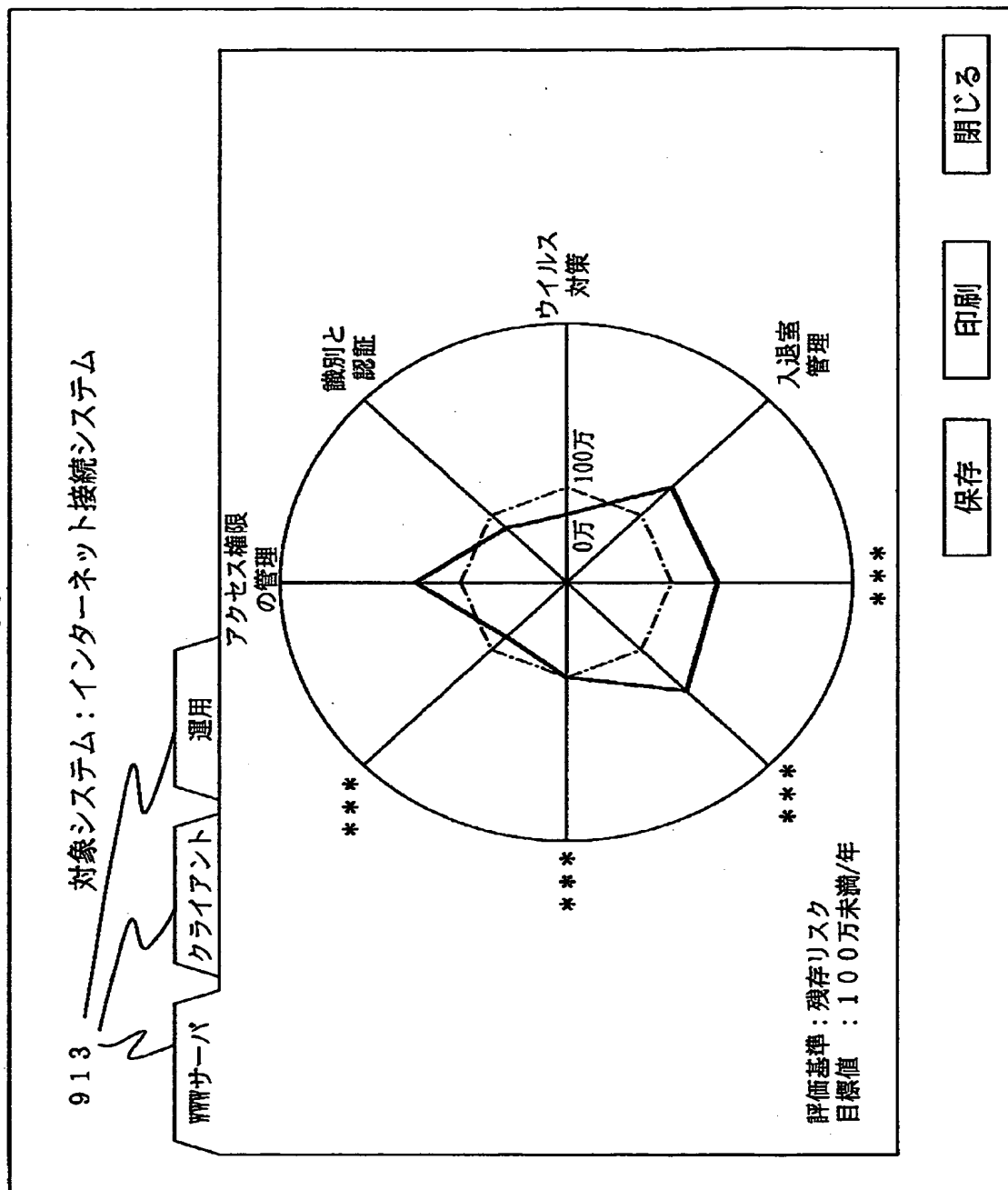
図13



【図 14】

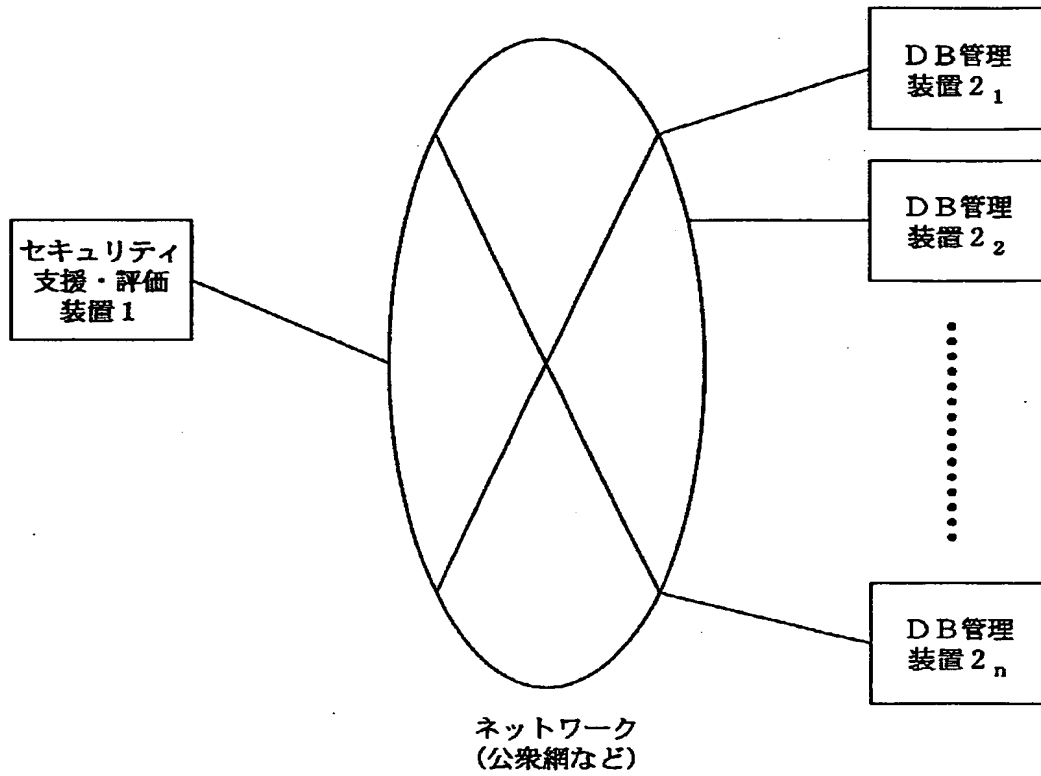


【図 15】

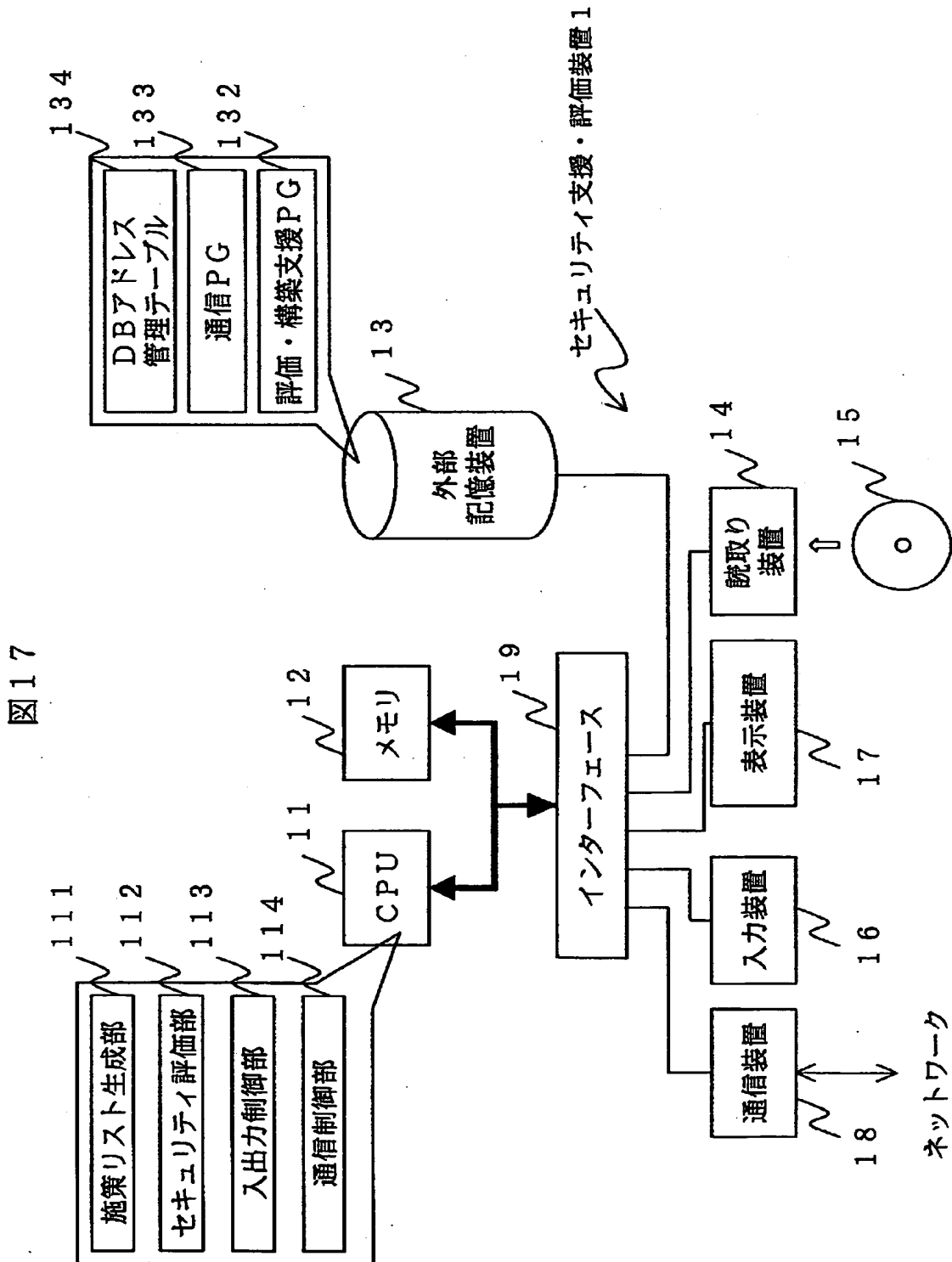


【図 1 6】

図 1 6



【図 17】



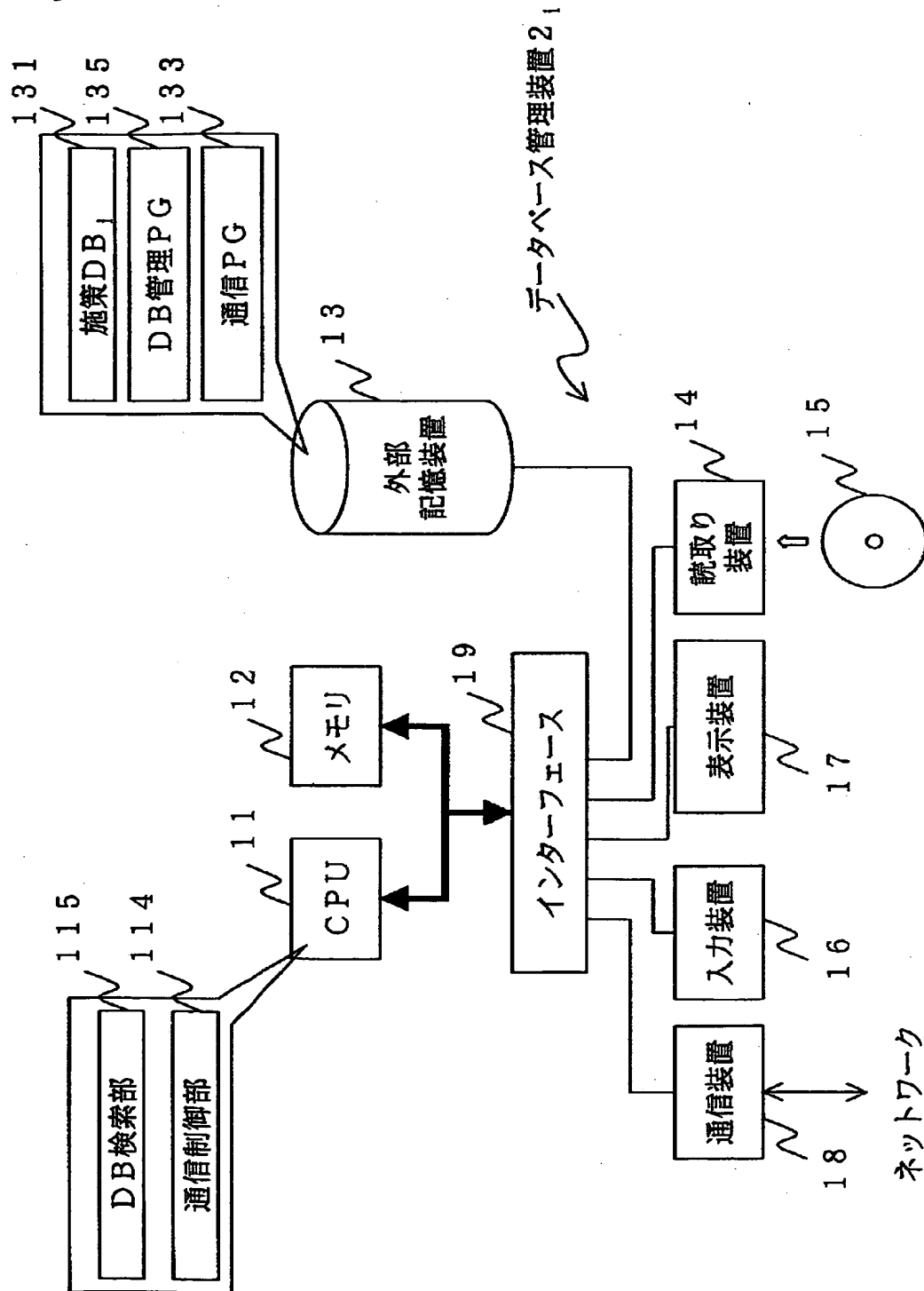
【図 1 8】

図 1 8

施策DB (対象システム)	DB管理装置アドレス
施策DB ₁ (インターネット接続システム)	****.***.**.**
施策DB ₂ (認証システム)	****.***.**.**
施策DB ₃ (プラントシステム)	****.***.**.**
⋮	⋮
施策DB _n (***システム)	****.***.**.**

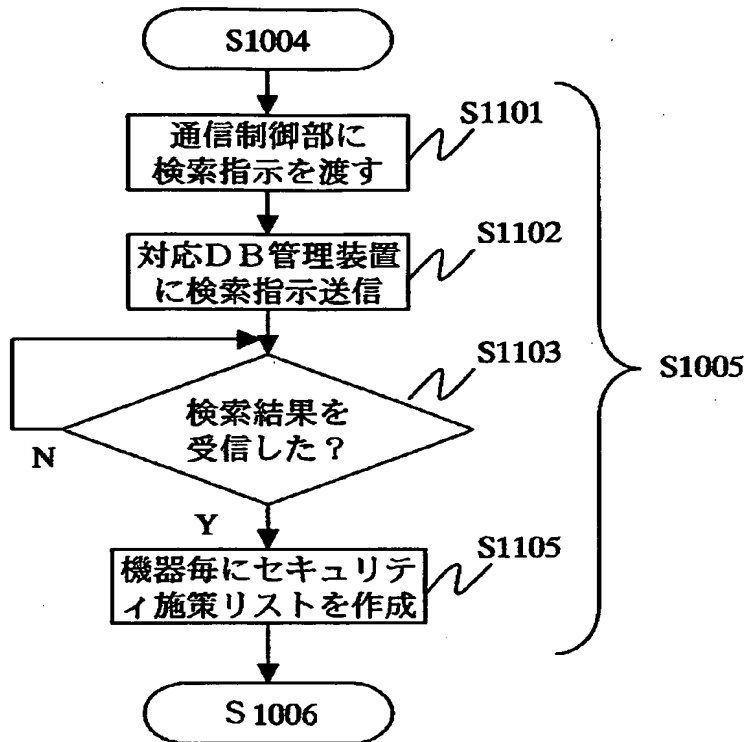
図 19

【図 19】



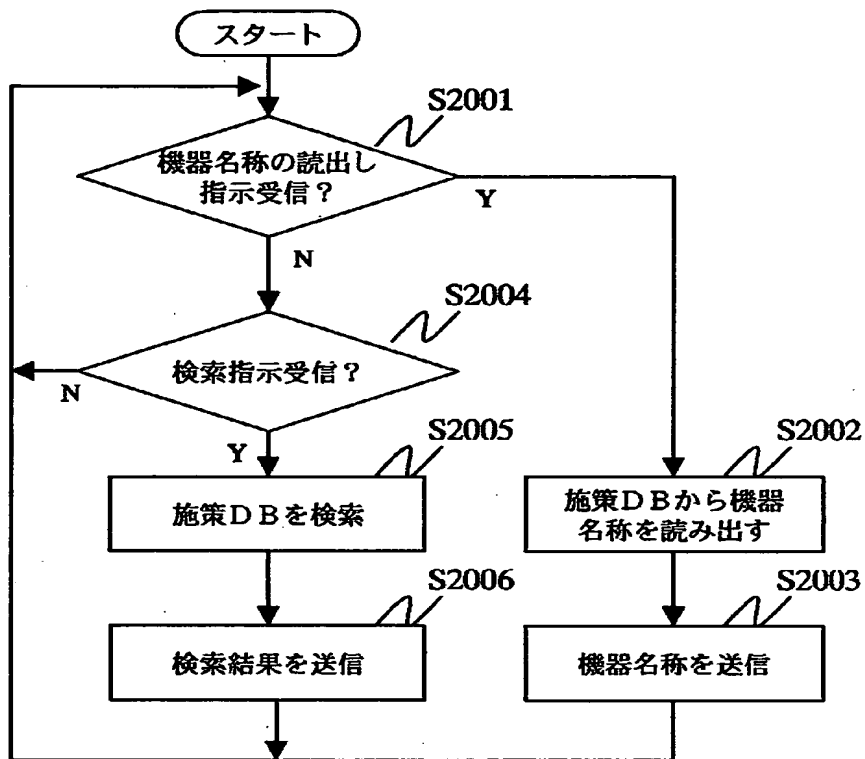
【図 2 0】

図 2 0



【図 2 1】

図 2 1



【書類名】 要約書**【要約】**

【課題】 高度な専門的知識がなくても、システムのセキュリティ状態を評価したり、セキュリティ施策の作成を支援することを可能にする。

【解決手段】 入力装置 1 6 を介して、操作者より評価対象システムと当該システムを構成する各機器の指定を受け付ける。次に、外部記憶装置 1 3 に格納されたセキュリティ施策データベース 1 3 1 を検索し、指定された評価対象システムの各機器に施すべきセキュリティ施策を読み出す。次に、指定された評価対象システムの機器毎に読み出したセキュリティ施策を対応付け表示装置 1 7 に表示し、入力装置 1 6 を介して、操作者よりセキュリティ施策の実施の有無を受け付ける。それから、受け付けた各機器のセキュリティ施策の実施の有無に基づいて、セキュリティ状態の評価を行ない、その結果を表示装置 1 7 に表示する。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [0 0 0 0 0 5 1 0 8]

1. 変更年月日 1 9 9 0 年 8 月 3 1 日

[変更理由] 新規登録

住 所 東京都千代田区神田駿河台 4 丁目 6 番地

氏 名 株式会社日立製作所